




Florida Department of Revenue
Office of Inspector General

Leon M. Biegalski
Executive Director

5050 West Tennessee Street, Tallahassee, FL 32399

floridarevenue.com

September 26, 2018

TO: Leon Biegalski, Executive Director
FROM: Sharon Doredant, Inspector General 
SUBJECT: Annual Report for Fiscal Year 2017/18

We are pleased to submit the Office of Inspector General's (OIG) Annual Report for the fiscal year ending June 30, 2018. This report is required by section 20.055(8), Florida Statutes, and reflects the major work activities of the Internal Audit, Internal Investigations, and Special Projects Sections.

We appreciate the confidence you have shown in this office and the cooperation and support of Department of Revenue (Department) management. We look forward to continuing our service to you, Department management and staff, and all Floridians by promoting accountability, integrity, and efficiency within the Department.

cc: Office of the Chief Inspector General
Office of the Auditor General

Department of Revenue Office of Inspector General

• INTERNAL AUDITS • INTERNAL INVESTIGATIONS • SPECIAL PROJECTS •



ANNUAL REPORT 2017-2018

TABLE OF CONTENTS

Executive Summary	1
Department of Revenue Vision, Mission, Values, and Guiding Principles	3
OIG Responsibilities	4
OIG Organizational Chart	5
Staff Training and Qualifications	6
Internal Audit Section	8
Internal Investigations Section	13
Special Projects Section	17
Appendix A	
Outstanding Corrective Actions for Prior Audit Reports	22
Appendix B	
Summary of Closed Internal Investigations for FY 2017/18	26

EXECUTIVE SUMMARY

Section 20.055 (8), Florida Statutes, (F.S.), requires the Office of Inspector General (OIG) to complete an annual report by September 30, summarizing the activities of the office during the prior fiscal year. This report must include, at a minimum:

- ◆ A description of activities relating to the development, assessment, and validation of performance measures.
- ◆ A description of significant abuses and deficiencies relating to the administration of programs and operations of the agency disclosed by investigations, audits, reviews, or other activities during the reporting period.
- ◆ A description of recommendations for corrective action made by the Inspector General during the reporting period with respect to significant problems, abuses, or deficiencies identified.
- ◆ The identification of significant recommendations described in previous annual reports on which corrective action has not been completed.
- ◆ A summary of audits and investigations completed during the reporting period.

The following activities highlight the significant efforts of the Department of Revenue (Department) OIG staff during Fiscal Year (FY) 2017/18:

Internal Audit Section

- ◆ Demonstrated compliance with applicable professional standards and the Code of Ethics issued by the Institute of Internal Auditors (IIA).
- ◆ Demonstrated general compliance with the provisions of s. 20.055, F.S., governing the operation of internal audit activities.
- ◆ Completed twenty-five projects:
 - ❖ Six audits
 - ❖ One consulting engagement
 - ❖ Twelve management services projects
 - ❖ Six response coordination activities
- ◆ Issued three management memorandums related to additional risks identified during service center audits.

Internal Investigations Section

- ◆ Updated policies and procedures, for implementation on July 1, 2018, to reduce the cycle time of cases and the overall time it takes to resolve complaints received by the section.
- ◆ Completed sixty-three cases:
 - ❖ Twenty investigations
 - ❖ Forty-three preliminary reviews
- ◆ Reduced amount of time to complete cases:
 - ❖ Decreased investigation time by forty-three percent
 - ❖ Decreased preliminary review time by thirteen percent

EXECUTIVE SUMMARY

Special Projects Section

- ◆ Completed seven fraud projects.
- ◆ Developed and delivered six instructor-led fraud awareness presentations.
- ◆ Developed and delivered a computer-based fraud awareness training module for all employees.
- ◆ Closed nineteen current arrest reviews.
- ◆ Reduced the average number of days to close current arrest reviews after a final order or other disposition by the court by forty-five percent.
- ◆ Assessed and responded to two hundred twenty workplace violence incident reports:
 - ❖ Two hundred three threats from external sources
 - ❖ Sixteen threats from internal sources
 - ❖ One threat from an unknown source

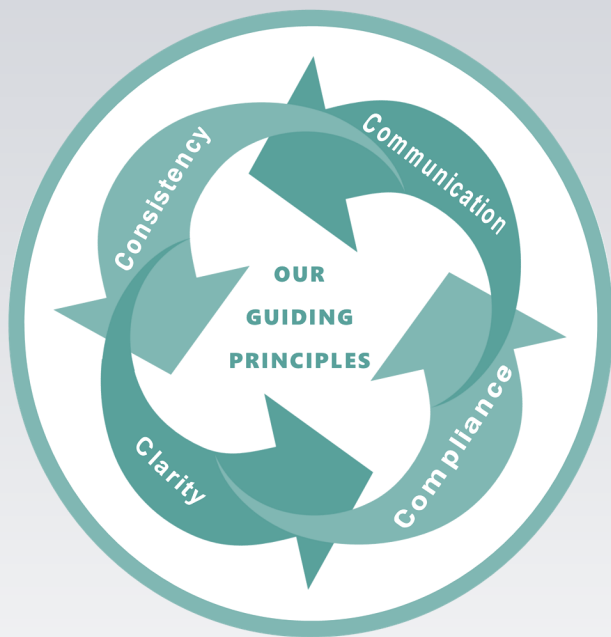
New Certifications

- ◆ Carol Matthews, Government Operations Consultant III in the Special Projects Section, earned the designation of Certified Fraud Examiner (CFE) by the Association of Certified Fraud Examiners, which required passage of the CFE Exam and possessing certain education and work experience in fraud related fields. Passing the CFE Exam required extensive self-study in the areas of financial transactions and fraud schemes, law, investigation, and fraud prevention and deterrence.
- ◆ Ruben Ramos and Sarah Bajoczky, Investigators in the Internal Investigations Section, earned the designation of Certified Inspector General Investigator (CIGI) by the Association of Inspectors General, which required completion of thirty-five hours of investigative training and passing an exam. The exam tested their knowledge in seven broad areas of core competency for inspector general investigators.
- ◆ Angela Welch, Deputy Inspector General, earned the designation of Certified Inspector General (CIG) by the Association of Inspectors General, which required completion of thirty-six hours of training and passing an exam. The exam tested knowledge in six broad areas of core competency for inspectors general.
- ◆ Cory Wilson, Computer Audit Analyst in the Internal Audit Section, passed the ISO/IEC 20000 Auditor exam and is now a certified ISO/IEC 20000 auditor. ISO/IEC 20000 is an international standard for information technology (IT) service management that promotes the adoption of an integrated process approach to the delivery of IT services to ensure satisfaction of customer requirements, cost-effectiveness, and smooth business processes.

DEPARTMENT OF REVENUE

VISION

An Agency that is accessible and responsive to citizens, provides fair and efficient tax and child support administration, and achieves the highest levels of voluntary compliance.



MISSION

To serve citizens with respect, concern, and professionalism;

To make complying with tax and child support laws easy and understandable;

To administer the laws fairly and consistently; and

To provide excellent service efficiently and at the lowest possible cost.

VALUES

Character values

- ◆ Integrity
- ◆ Honesty
- ◆ Trust
- ◆ Fairness
- ◆ Respect
- ◆ Concern for others

- ◆ Service
- ◆ Excellence
- ◆ Innovation
- ◆ Commitment
- ◆ Communication
- ◆ Teamwork
- ◆ Knowledge

Performance values

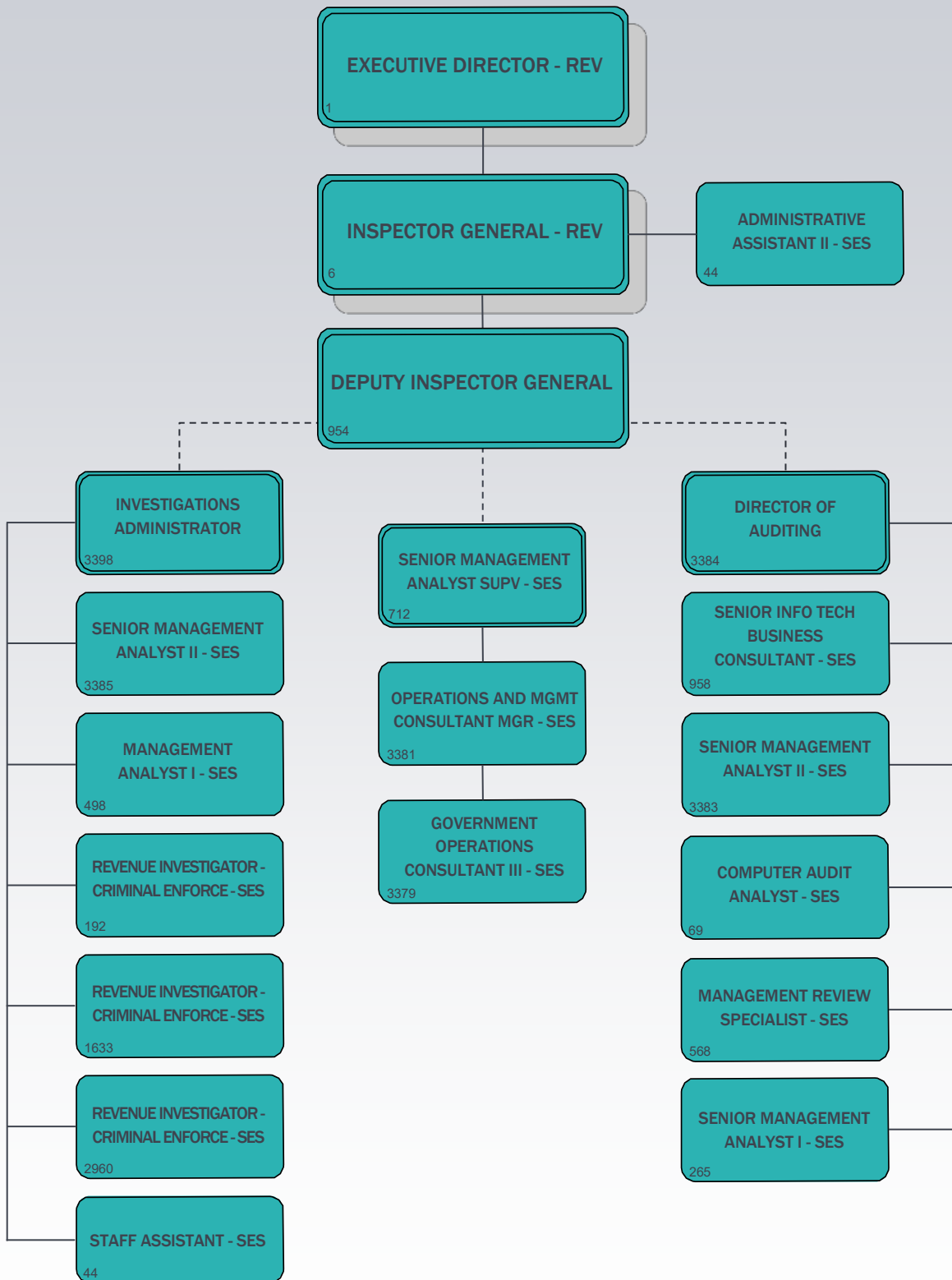
OIG RESPONSIBILITIES

Section 20.055(2), F.S. states, in part, “An office of inspector general is established in each state agency to provide a central point for coordination of and responsibility for activities that promote accountability, integrity, and efficiency in government.” Responsibilities of each Inspector General, as defined in s. 20.055, F.S., are reflected in the following table.

		PROMOTE			
EFFICIENCY	Informing and updating the Executive Director of fraud, abuses, and deficiencies concerning program operations; recommending corrective action; and monitoring progress made in corrective action.		Conducting, supervising, or coordinating activities to prevent and detect fraud and abuse and promote economy and efficiency in the administration of programs and operations.		INTEGRITY
	Directing, supervising, and coordinating audits, investigations, and management reviews relating to the programs and operations of the Department.		Assessing the reliability and validity of the information provided on performance measures and standards, and recommending improvements.		
	Ensuring effective coordination and cooperation with the Auditor General, federal auditors, and other governmental bodies.	Reviewing actions taken by the Department to improve program performance and meet standards.	Reviewing rules, as appropriate, relating to the programs and operations of the Department.	Complying with General Principles and Standards for Offices of Inspector General.	
	Ensuring an appropriate balance is maintained between audit, investigative, and other accountability activities.		Advising in the development of performance measures, standards, and procedures for the evaluation of Department programs.		
		ACCOUNTABILITY			

The OIG is responsible for internal audits, internal investigations, fraud prevention and response, and special projects as directed by the Inspector General. These responsibilities are carried out by 19 full-time equivalent positions. The OIG is in the Executive Direction and Support Services Program (EXE), and the Inspector General reports directly to the Executive Director. The OIG’s seasoned and exemplary staff strives to provide the Executive Director and other Department leaders with timely information to improve operations, champion integrity, and ensure the security of Department employees and information. They exemplify the best of public service and work hard to accomplish this mission.

OIG ORGANIZATIONAL CHART



STAFF TRAINING AND QUALIFICATIONS

Section 20.055, F.S., requires the OIG to comply with the *General Principles and Standards for Offices of Inspector General* as published and revised by the Association of Inspectors General. These standards require OIG staff to obtain a minimum of 40 hours of continuing professional education every two years.

OIG staff backgrounds and experience cover a wide variety of disciplines including:

- ◆ Accounting
- ◆ Auditing
- ◆ Investigations
- ◆ Crime prevention
- ◆ Information systems
- ◆ Fraud prevention and detection



OIG staff participated in courses, conferences, seminars, and webinars made available through the Association of Inspectors General, the Association of Certified Fraud Examiners, the Institute of Internal Auditors, the Association of Governmental Accountants, and other national organizations and vendors who provide training focused on audit, investigation, fraud, data analytics, and workplace violence.

During FY 2017/18, staff received training in the following areas:

- ◆ Conducting Equal Employment Opportunity Commission investigations
- ◆ Advanced investigative interviewing
- ◆ Investigating sexual harassment allegations
- ◆ Fraud risk management
- ◆ Data analytics
- ◆ Internal controls
- ◆ Engagement process
- ◆ Florida Single Audit Act
- ◆ Green Book implementation – Leading practices for state and local governments
- ◆ Auditing performance management systems
- ◆ Advance accountability, contract/grant management and monitoring
- ◆ Audit evidence and workpapers
- ◆ IT Auditing
- ◆ Networks, operating systems and cyber security
- ◆ Conducting advanced IT auditing engagements



Fifteen staff employed during FY 2017/18 maintained professional certifications

STAFF TRAINING AND QUALIFICATIONS

Staff members have professional certifications and participate in many professional organizations to maintain proficiency in their profession.

Below is a summary of professional certifications maintained by OIG staff members and the professional organizations in which they participate.

Certifications

- ❖ Florida Crime Prevention through Environmental Design Practitioner (FCP)
- ❖ Florida Crime Prevention Practitioner (FCPP)
- ❖ Certified Fraud Examiner (CFE)
- ❖ Certified Government Auditing Professional (CGAP)
- ❖ Certified in Financial Forensics (CFF)
- ❖ Certified Information Systems Auditor (CISA)
- ❖ Certified Information Systems Security Professional (CISSP)
- ❖ Certified Inspector General (CIG)
- ❖ Certified Inspector General Auditor (CIGA)
- ❖ Certified Inspector General Investigator (CIGI)
- ❖ Certified Internal Auditor (CIA)
- ❖ Certified Internal Control Auditor (CICA)
- ❖ Certified Public Accountant (CPA)
- ❖ Certified Public Manager (CPM)
- ❖ Internal Auditor Certification in Information Technology Systems Management According to ISO/IEC 20000-1:2011
- ❖ Six Sigma Yellow Belt Certified

Professional Organizations

- ❖ American Institute of Certified Public Accountants
- ❖ Association of Certified Fraud Examiners
- ❖ Florida Chapter of the Association of Inspectors General
- ❖ Institute of Internal Auditors
- ❖ Internal Controls Institute
- ❖ ISACA (Formerly known as Information Systems Audit and Control Association)
- ❖ National Association of Inspectors General
- ❖ North Florida Certified Public Managers Chapter
- ❖ Tallahassee Chapter of the Institute of Internal Auditors
- ❖ Tallahassee Chapter of the Association of Certified Fraud Examiners

INTERNAL AUDIT

The OIG is responsible for conducting financial, compliance, IT, and performance audits, as well as management reviews relating to the programs and operations of the Department in accordance with sections 20.055 (2)(d) and 20.055(6), F.S. Additionally, the Internal Audit Section (IAS) reviews and evaluates internal controls necessary to ensure the Department's fiscal accountability. Engagements are performed under the direction of the Director of Auditing.

IAS performs audits (assurance engagements) and consulting engagements in accordance with the *International Standards for the Professional Practice of Internal Auditing (Standards)*, published by the IIA, and the *Principles and*

Standards for Offices of Inspector General, published by the Association of Inspectors General. Specifically, the internal audit activity governs itself by adherence to IIA's mandatory guidance contained in the *International Professional Practices Framework (IPPF)*, which includes the "Core Principles for the Professional Practice of Internal Auditing," the "Code of Ethics," the "International Standards for the Professional Practice of Internal Auditing," and the "Definition of Internal Auditing." IIA's mandatory guidance constitutes the fundamental requirements for the professional practice of internal auditing.

Definitions and Requirements

According to the *Standards*:

- ◆ Assurance engagements are an objective examination of evidence to provide "an independent assessment on governance, risk management, and control processes for the organization."
- ◆ Consulting engagements are advisory client services activities and may be formal or informal.
 - ❖ Formal consulting engagements are generally performed at the request of executive or program management.
 - ❖ Informal consulting engagements generally involve reviews of internal controls, performance measures, or policies and procedures, and may include other activities such as participation on teams or assisting in an internal investigation.

The *Standards* also require auditors to follow up on reported findings and recommendations from previous audits to determine whether management has taken prompt and appropriate corrective action. This includes monitoring responses and planned corrective actions to findings and recommendations made in reports issued by the Office of the Auditor General and the Office of Program Policy Analysis and Government Accountability, as required by s. 20.055(6)(h), F.S. Every six months, IAS requests status updates from management about the progress of corrective action plans and verifies corrective actions resolved the issues on any findings management reported as completed.



There is a difference in terminology between Florida Statutes (audits) and the *International Standards for the Professional Practice of Internal Auditing*, published by the Institute of Internal Auditors (assurance engagements). For brevity, the term "audit" will be used in this document except in sections specifically referencing the *Standards*.

INTERNAL AUDIT

Accomplishments



- ◆ Issued three management memorandums related to risks identified during a service center audit.
- ◆ Provided training to new supervisors within the Department about the importance of internal controls.
- ◆ Completed training that will enhance the efficiency and effectiveness of the internal audit function.

Audit Engagements

During FY 2017/18, IAS completed six audits. Below is a summary of the objectives for each of the audits. For related recommendations that were open as of June 30, see Appendix A.

1. Child Support Program Payment Processing and Fund Distribution—Revenue Processing

The objective of the audit was to determine whether selected internal controls for processing collections received by the Revenue Processing sub-process are adequate to ensure receipts are properly safeguarded, recorded, and deposited.

2. Agency-wide Software Purchasing

The objectives of the audit were to determine whether:

- ◆ Software purchasing throughout the Department is efficient and effective.
- ◆ Selected internal controls for software purchases throughout the Department are adequate to ensure software products are tracked and maintained in compliance with Florida Cybersecurity Standards, as specified in Rule 74-2, Florida Administrative Code (F.A.C.).

3. Agency-wide Hiring Practices

The objectives of the audit were to determine if Department procedures related to Veterans' Preference are adequate and if they are being followed when filling career service vacancies.

4. Agency-wide Family and Medical Leave Act (FMLA), Americans with Disabilities Act (ADA), and Sick Leave Pool (SLP) Process

The objective of the audit was to determine if the Department's FMLA, ADA, and SLP programs are effectively coordinated.

INTERNAL AUDIT

5. Service Centers

The objectives of the audit were to determine:

- ◆ The adequacy of payment processing procedures
- ◆ The adequacy of monitoring and accounting for attractive inventory items
- ◆ Whether controls associated with information security are adequate and effective
- ◆ Whether physical security controls are sufficient to protect assets

6. Agency-wide Multi-Functional Devices (MFDs)

The objective of the audit was to determine whether internal controls ensure compliance with requirements in Rule 74-2, F.A.C., and Internal Revenue Service Publication 1075, that govern the installation, configuration, and removal of MFDs.



Consulting Engagements

IAS completed one consulting engagement during FY 2017/18:

ISO 20000 Internal Audit 2017/18

The purpose of the engagement was to assist the Information Services Program (ISP) by conducting a review in accordance with the International Organization for Standardization (ISO). ISO 20000 is a set of international standards recognized in the information technology industry. The annual review identifies opportunities for improvement and allows ISP to begin making those improvements before an external audit is conducted.

NOTE: In the past, an outside consultant conducted the ISO 20000 review.



By performing this function, IAS saved the Department approximately \$16,000.

INTERNAL AUDIT

Summary of Activities

Review of Performance Measures

In accordance with s. 20.055(2)(a), F.S., the OIG serves in an advisory capacity to program management and staff during the development of performance measures, standards, and procedures for the evaluation of the Department's programs. Additionally, IAS reviews and verifies the validity and reliability of related performance measures during assurance engagements performed during the year.



Annual Risk Assessment Activities

IAS staff met with the programs and executive management to facilitate identification of areas with the highest levels of risk exposure. Criteria used for the risk assessment included complexity of operations, management interest, controls, financial materiality, changes in procedures and personnel, results of prior audits, public exposure, and potential for fraud. Results from the risk assessment are used to develop IAS's long-term and annual audit plans.

Florida Single Audit Act Activities

IAS staff acted as agency coordinator for the Florida Single Audit Act (FSAA). IAS acted as liaison with program FSAA leads, helped identify legislative effects on the Department related to the FSAA, and handled inquiries from the public or other state agencies. IAS was also responsible for the annual certification of the Department's FSAA projects to the Department of Financial Services.

Opa-locka Financial Emergency Board Participation

The Governor appointed the Director of Auditing to serve on the Opa-locka Financial Emergency Board, which was established through Executive Order Number 16-135 pursuant to s. 2018.503(1), F.S. The purpose of the Financial Emergency Board is to oversee the City of Opa-locka financial activities and provide technical assistance.

Follow-Up on Corrective Action Plans as of 6/30/2017

The purpose of this review was to follow up on the programs' assertions for the corrective action plans as of June 30, 2017. A summary report provided to the Executive Director reflected 33 open findings, 17 findings verified by OIG staff as closed during the period, and 16 corrective actions overdue.

Follow-Up on Corrective Action Plans as of 12/31/2017

The purpose of this engagement was to follow up on program assertions for corrective action plans as of December 31, 2017. A summary report provided to the Executive Director reflected 25 open findings, 11 findings verified by OIG staff as closed during the period, and 13 corrective actions overdue.



See Appendix A for a list of the Outstanding Corrective Actions for Prior Audit Reports.

INTERNAL AUDIT

Other Services

Other IAS services include:

- ◆ External audit coordination
- ◆ Management services

During FY 2017/18, IAS staff coordinated six external audits conducted by other entities and the Department's responses to those audits when necessary.

Management services consist of various monitoring activities and special projects requested from management. These activities can be planned or unplanned. When management requests a special project, OIG management evaluates whether IAS has available resources and sufficient expertise to perform the engagement.



INTERNAL INVESTIGATIONS

Section 20.055(7), F.S., requires the Inspector General to “initiate, conduct, supervise, and coordinate investigations designed to detect, deter, prevent, and eradicate fraud, waste, mismanagement, misconduct, and other abuses” in the Department. The statutorily required investigative duties and responsibilities of the Inspector General, include:

- ◆ Receiving complaints and coordinating all activities required by sections 112.3187–112.31895, F.S., (the Whistle-blower’s Act) for the Department.
- ◆ Receiving and considering complaints which do not meet the criteria for an investigation under the Whistle-blower’s Act and conducting, supervising, or coordinating such inquiries, investigations, or reviews when appropriate.
- ◆ Promptly reporting to the Florida Department of Law Enforcement or other law enforcement agencies, as appropriate, when there are reasonable grounds to believe there has been a violation of criminal law.
- ◆ Conducting investigations and other inquiries free of actual or perceived impairment to the independence of the Inspector General or the OIG. This includes freedom from any interference with investigations and timely access to records and other sources of information.



- ◆ Submitting timely reports to the Department’s Executive Director regarding investigations conducted, except for whistle-blower investigations, which are reported as required by s. 112.3189, F.S.

The Internal Investigations Section (IIS) is responsible for conducting internal investigations to resolve allegations of violations of the Department’s conduct standards and other policies, rules, directives, and laws impacting the Department. Investigations may be initiated because of information received from:

- ◆ Department employees
- ◆ Private citizens
- ◆ Other state or federal agencies
- ◆ The Whistle-blower’s Hotline

IIS staff review each complaint received by the section. The review process filters complaints to ensure investigative resources are used effectively and efficiently.

Established criteria are used to evaluate each complaint to determine the appropriate course of action. When the review determines that a full investigation is warranted, an investigation is initiated.

Most allegations investigated involve violations of the Department’s *Standards of Conduct* such as:

- ◆ Breaches of confidentiality
- ◆ Employment discrimination
- ◆ Falsification of records
- ◆ Inappropriate e-mail or Internet transactions
- ◆ Misuse of state property
- ◆ Theft

Investigations may result in management issuing the employee disciplinary action, up to and including dismissal. IIS also refers information and provides assistance to local, state, and federal law enforcement agencies on cases related to possible criminal violations or activities.

INTERNAL INVESTIGATIONS

Accomplishments



IIS established a process improvement team to identify efficiencies in processing complaints.



The team made recommendations to streamline activities performed within the intake process. The team's recommendations were approved by the Inspector General and reflected in the section's updated policies and procedures implemented on July 1, 2018. The modified process should reduce the overall time it takes to resolve complaints received by the section.

Highlights of worked performed

A number of significant preliminary reviews and investigations were conducted during FY 2017/2018. The following are highlights of some of these cases:

Theft



The OIG received information from the Federal Bureau of Investigation (FBI), that an employee accessed confidential information for unauthorized purposes and released personally identifiable information to be used for purposes contrary to the law. The employee was interviewed and admitted obtaining personally identifiable information from information systems the employee was authorized to access for his or her job, and providing it to individuals to use for unlawful personal gain. Additionally, during the investigation, it was discovered the employee failed to disclose a prior arrest on his or her State of Florida employment application, and as a result the employee's employment with the Department was terminated. The former employee was adjudicated guilty of criminal charges, received a twenty-seven month prison sentence followed by 3 three years of supervised release, and was required to pay several thousand dollars in restitution.

Employment Discrimination

The Department's Discrimination Intake Officer referred a complaint to the OIG from an employee who alleged race discrimination. The employee alleged being treated differently by management related to leave requests, work assignments, job performance, and recognition. The review determined the employee did not provide sufficient information to support the allegations of race discrimination. It also found the employee misrepresented his or her need to use accrued personal leave to Management.

INTERNAL INVESTIGATIONS

Gifts and Gratuities from Outside Sources

The OIG received an allegation from management based upon an anonymous complaint that an employee accepted a gift from a child support customer. During the investigation, the employee admitted to accepting the gift and taking it home, but said the gift was later returned to the office to provide to charity. The investigation could not determine if the gift-giver was a child support customer or had any relationship to or with the Department. As a result, there was insufficient information to support the employee violated the Department's gift policy. However, the investigation supported a finding the employee did not contact the Department's Ethics Officer for guidance prior to accepting the gift and the employee's action of accepting the gift created the appearance of impropriety. The employee received corrective action.



Confidentiality

The OIG received an allegation that an employee accessed and viewed records in the Department's information systems for nonwork-related reasons. The investigation determined that, in addition to accessing information systems for purposes not related to work, the employee intentionally entered incorrect purpose codes in the information systems to perform the unauthorized record searches. The employee also failed to receive approval from the Department for his or her personal business, made a status change for the personal business account in the tax system, and failed to timely file the business's sales and use tax returns. Finally, the employee failed to follow his or her supervisor's instructions when the employee continued to access the information systems for nonwork-related reasons. The Department terminated the employee's employment as a result of the findings of the investigation.



Conflict of Interest-Personal Relationships

Management referred an allegation received from a child support customer to the OIG. The customer alleged that an employee helped a person owing child support avoid sanctions for not paying support. The investigation determined the employee created multiple written agreements with the person owing support while in a personal relationship with the person, accessed and viewed confidential records in the Department's information systems related to the same person, was untruthful with management when questioned about the personal relationship, and failed to disclose conflict cases relating to the person to management. The Department terminated the employee's employment.



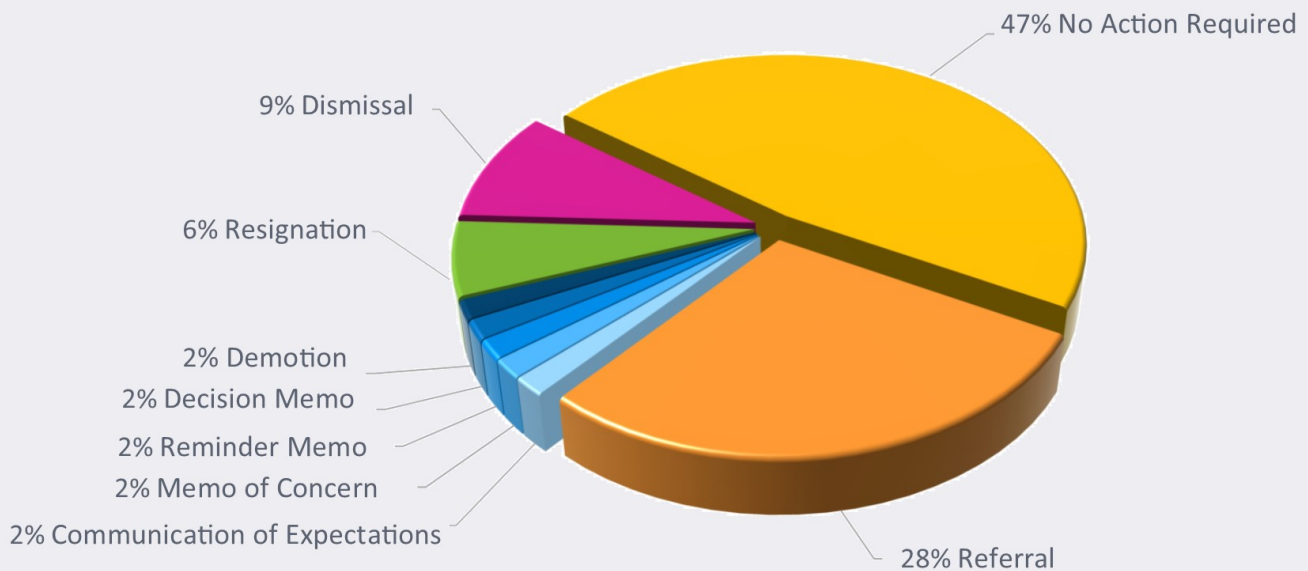
See Appendix B for a summary of closed cases FY 2017/18, including data from both preliminary reviews and investigations.

INTERNAL INVESTIGATIONS

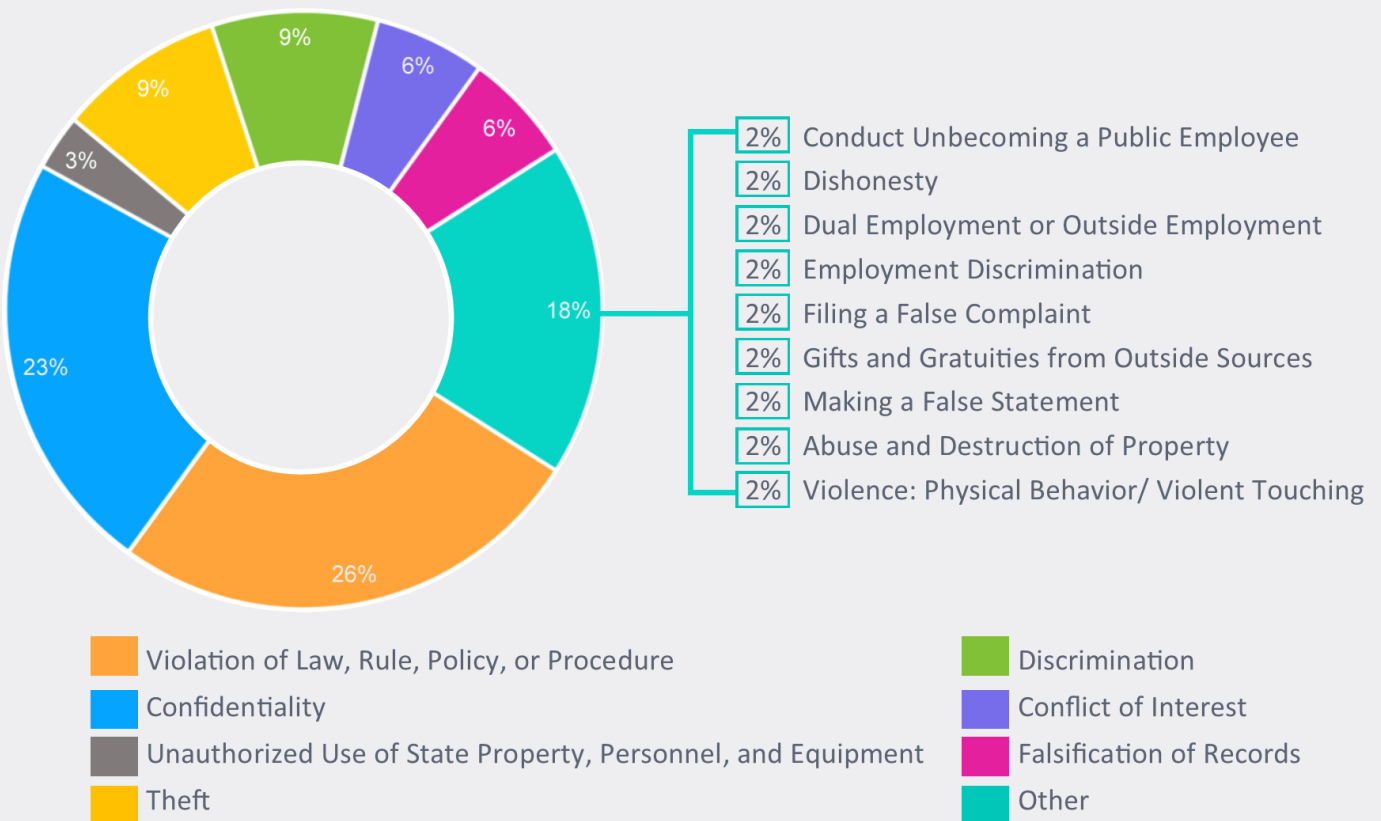
Information on Closed Internal Investigations for FY 2017/18

NOTE: The charts include data from both preliminary reviews and investigations.

Final Disposition of Closed Cases



Cases Closed by Type



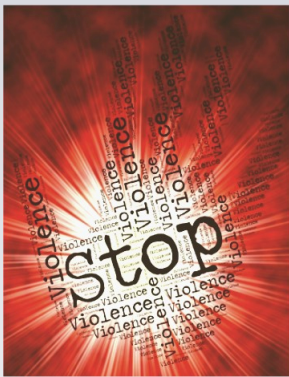
SPECIAL PROJECTS

The Special Projects Section (SPS) is assigned various responsibilities. These responsibilities include programs related to:

- ◆ Workplace violence prevention and response
- ◆ Employees' reports of current arrests
- ◆ Fraud prevention and response
- ◆ Risk assessments of proposed and revised agency policies

SPS's goals are to provide a work environment for Department employees free from fear of violence, foster a culture of fraud awareness and prevention within the Department, and provide management with information necessary to ensure a desired level of integrity among Department staff.

Workplace Violence



The Department's workplace violence policies and procedures emphasize protecting employees from all forms of workplace violence, including assaults and threats from external customers, domestic violence affecting the workplace, and incidents of violent behavior between employees. The Department's *Workplace Violence Prevention and Response Policy*, which also addresses domestic violence affecting the workplace, requires the reporting of all incidents or threats of workplace violence to the OIG. Local law enforcement or other appropriate responders are notified when necessary to respond to a workplace violence incident. SPS staff ensures all potentially affected managers at the agency, program, region, and service center levels are timely notified of reported incidents and provides recommendations for appropriate action.

Workplace violence can originate from internal or external sources. Most reported workplace violence incidents reported to the OIG originate from external sources. External workplace violence incidents include assaults and threats made by customers against Department employees as a result of their official duties. Generally, threats against employees are reported to a local law enforcement agency with jurisdiction where the threat was made.

External sources of workplace violence also include threats made or reported to the Department by a customer, but directed toward someone else, such as a parent owing support in a child support case threatening to harm the parent owed support or a child in the case. The *Workplace Violence Prevention and Response Policy* requires that Department staff notify local law enforcement of the threat and attempt to notify the person who the threat was directed toward, so they can determine the most appropriate action to provide for their safety.

Altercations between customers while on Department property that don't directly involve Department employees are also reported as external sources of workplace violence. These types of incidents could escalate and endanger Department employees and other customers. Generally, local law enforcement is called to respond to these types of incidents.

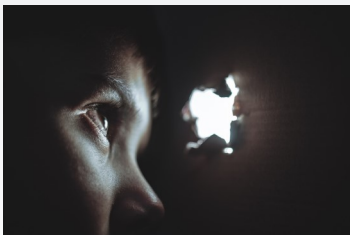
SPECIAL PROJECTS

Threats of suicide made by customers to Department employees are also reported to and logged by SPS as an external source of workplace violence. Response may include notifying local law enforcement in the area where the person making the threat lives and requesting a wellness check on the individual who made the suicide threat.

When it is determined that a potentially violent person may be associated with a tax account or child support case, a Potentially Dangerous Contact (PDC) indicator is placed on applicable primary databases used within the Department's operating programs. The PDC indicator serves as notice to an employee that special care should be taken in any contact or action on the account. SPS staff is available to assist the operating programs in determining appropriate action to help ensure the safety of staff while also helping to ensure the Department's statutory tax and child support administration responsibilities are carried out in relation to an account flagged as a PDC.



Internal workplace violence incidents occur when an employee or contractor's employee feels threatened or endangered due to the actions or statements of another employee or contractor's employee. Internal workplace violence incidents are generally addressed by assembling the Department's Workplace Violence Response Team (WPV Team). The WPV Team consists of the Inspector General, the SPS Manager, the Employee Relations Manager, and the Chief Assistant General Counsel for the Executive Program. The WPV Team works cooperatively to determine and advise management of the recommended response to reported incidents. The WPV Team's recommendation(s) to management may include disciplinary action, counseling, referral to the Employee Assistance Program (EAP), or other mitigating action. The WPV Team may also request an internal investigation if facts of the incident cannot be determined.



Domestic violence affecting the workplace is a concern for any agency or business. A domestic violence concern can be initiated by an external or internal source. The Department's *Standards of Conduct* require any employee who is named as the respondent in an injunction for protection against domestic violence, or any similar injunction, where the petitioner is also a Department employee, to report the injunction to the OIG. The

Department's *Workplace Violence Prevention and Response Policy* encourages employees to report if they are the petitioner in an injunction for protection against domestic violence and they have any concern that the respondent may come to the workplace. SPS works with appropriate management to take necessary actions to help protect victims of domestic violence in the workplace, as well as to help ensure the safety of co-workers. The WPV Team may be convened if needed to address more serious incidents of domestic violence affecting the workplace.

SPECIAL PROJECTS

Current Arrests

SPS is responsible for receiving and following up on reports of current employees who are arrested or charged with criminal offenses.

The Department's *Standards of Conduct* require that employees timely report the following events to the OIG:

- ◆ Any arrest, charge, or receipt of a Notice to Appear for a crime that is punishable by more than sixty days' imprisonment and/or more than a \$500 fine
- ◆ The final order or other disposition of an arrest or charge for a crime that is punishable by more than sixty days' imprisonment and/or more than a \$500 fine
- ◆ The resolution of an outstanding arrest warrant
- ◆ Being named as the respondent in an Injunction for Protection against Domestic Violence or any similar injunction, where the petitioner is also a Department employee



When a report is received from an employee or other source, SPS staff will notify the program director for the employee's program so they can determine any conflict with employment and ensure staff integrity. SPS will also open a review file to monitor court actions and ensure the employee meets all reporting requirements established in the Department's *Standards of Conduct*.

When the final disposition of the charge(s) is entered by the court, program management is notified of the outcome of the criminal case and whether the employee complied with reporting requirements. Program management may issue corrective action based on an employee's failure to timely report an arrest or the final disposition of a charge, and/or the nature of the offense and how it affects the employee's ability to perform assigned duties.

SPS Accomplishments

Arrest review time decreased by **45%** compared to prior fiscal year

Worked **7** fraud review projects

Delivered **7** fraud awareness presentations

Closed **19** current arrest reviews

Timely assessed **220** Workplace violence reports

Developed a risk-based fraud work plan

SPECIAL PROJECTS

Fraud Prevention Program



SPS is responsible for developing and implementing programs to aid in the prevention, deterrence, and detection of fraud within the agency. The Department's *Fraud Prevention and Response Policy*, developed by SPS staff and adopted by the agency in 2014, provides clear guidance to management and employees on actions to take if they suspect fraudulent activity within or affecting Department services.

SPS staff continue to champion the agency-wide fraud prevention and response program. This year, to improve the efficiency and effectiveness of the fraud program, SPS developed and implemented an annual risk-based fraud work plan and a time accounting system to capture direct and indirect project time.

SPS's focus this year was on raising employee fraud awareness. SPS began the year by releasing a web-based fraud awareness training module, delivered as mandatory for all employees via the Department's Learning Management System (LMS). The training was followed up by a rollout of activities associated with National Fraud Awareness Week. SPS distributed the Governor's proclamation and a fraud awareness week poster developed by the Association of Certified Fraud Examiners (ACFE) to all managers for posting throughout the Department. An agency-wide communication was also distributed to inform all Department staff of National Fraud Awareness Week and remind them of their responsibility to complete the fraud awareness training in LMS.

Six instructor-led training sessions were delivered:

- ◆ Three fraud awareness presentations to new supervisors
- ◆ Presentation to Child Support service center managers and administrators, focusing on "red flags" specific to child support
- ◆ Presentation to internal audit staff on considering fraud during audit engagements
- ◆ Presentation to the Child Support Council on conducting a fraud risk assessment for their business processes



SPS responsibilities include looking globally at departmental data to perform data analysis. Anomalies are referred to the internal audit or internal investigations sections for further review. When appropriate, referrals are made to law enforcement and other applicable agencies.

SPECIAL PROJECTS

Highlights of worked performed

The following are highlights of some of the projects performed and a summary of the most significant issues identified by SPS staff during FY 2017/18:

Limiting Access to Social Security Numbers



SPS identified a Department-developed application to search for employees' social security numbers, to facilitate the reconciliation of financial transactions in FLAIR. Recommendations were made to remove the application, and to delete social security numbers from reports and other documents provided to Department staff by the Department's Office of Financial Management, unless a specific business need for providing the social security numbers was identified.

Driver's License Suspensions

Data on user initiated driver's license suspensions and reinstatements were reviewed to identify potential fraud. A memo identifying some potential weaknesses in controls was provided to Child Support program management, who responded that procedures would be revised and CAMS would be updated to address the concerns.

Potential Mail Fraud

Department mailroom staff were informed by local post office staff in Tallahassee that a customer was attempting to have Department mail re-routed to a residential address. After meeting with Tallahassee post office staff, the concern was referred to Postal Inspections staff in West Palm Beach, who identified that the individual was also attempting to re-route mail from three other locations. Postal staff confirmed that a business address should not be changed to a residential address by a private individual. Postal Inspections staff and local law enforcement determined there was no criminal intent. SPS staff worked with postal staff to ensure receipt of all Department mail.



APPENDIX A

Outstanding Corrective Actions as of June 30, 2018

Project #	Audit Name	Recommendation(s)
2012-0115	Department-wide Data Security	One confidential outstanding corrective action
2013-0106	Agency Information Technology Security Governance	One confidential outstanding corrective action
2014-0126	Agency Information Security Management – Service Centers	One confidential outstanding corrective action
2015-0126	Child Support Program (CSP) - Payment Processing and Fund Distribution, Revenue Processing	Management should revise procedures to include missing control elements.
		Management should take steps to ensure the deposit pick-up area is secure.
		Management should request access to data necessary to monitor segregation of duties.
		Management should ensure that security roles with segregation of duties in the Enterprise Central Component system are working as intended.
		Management should develop a plan for processing payments on days when Revenue Processing is short-staffed.
2016-0101	Agency-wide Software Purchasing	The Information Services Program (ISP) should work with the Office of Financial Management (OFM) to ensure agency-wide procedures governing software purchases are adequate to support ISP's primary functions. At a minimum, the procedures must be clear and consistent, and define software-related terms. Additionally, the procedures should specify approval requirements, including ISP delegations of approval.
		ISP should work with OFM to review commodity codes and object codes to determine which should be routed for IT approval. Additionally, ISP should determine whether efficiency could be improved by removing the need for a separate STAIRS ticket and approving all IT software purchases using My Florida Marketplace's built-in approval flow.
		The Department should implement a software asset management (SAM) system to assess agency-wide software needs and coordinate enterprise-wide software purchases.
		Executive Leadership should ensure ISP devotes adequate resources to develop and implement a SAM system, including agency-wide SAM policies, processes, and procedures that comply with requirements of Rule 74-2, F.A.C.
		The Department should monitor software installations to identify uncategorized software, block the installation of unauthorized software, and ensure removal of unauthorized software installations.
		The Department should ensure that software is properly documented.

APPENDIX A

Project #	Audit Name	Recommendation(s)
2016-0106	Agency-wide Hiring Practices	<p>Office of Workforce Management (OWM) Talent and Growth Management should revise Department Policy DOR-1080-034B, Veterans' Preference Policy, to include "absolute preference" for veterans who have passed a skills verification test and are 30% or more disabled and the requirement to enter the names of preference eligible veterans on an appropriate register or list in accordance with their respective augmented ratings, as required by s. 295.08, F.S. In addition, OWM Talent and Growth Management should:</p> <ul style="list-style-type: none"> a. Revise the Human Resources website, Veterans' Preference in the Hiring Process Step 5 Skills Verification Test, to include the requirement to enter the names of preference eligible veterans on an appropriate register or list. b. Adopt the Department of Management Services (DMS) <i>Policy Guideline, Administration of Veterans' Preference in the Career Service</i>, scoring and rating template to be included as a ranking tool in the Veterans' Preference in the Hiring Process Step 5 Skills Verification Test. c. Revise the Selection Package Retention Process to require all Veteran's Preference candidates' ranking documentation be included with the Selection Package. <p>OWM Talent and Growth Management should revise internal procedures to include a quality assurance review element to ensure packages include all Veteran's Preference documentation.</p> <p>OWM Talent and Growth Management should implement a quality review related to Veterans' Preference.</p> <p>When necessary, OWM Talent and Growth Management should provide additional training to hiring managers.</p>
2017-0109	Agency-wide Family and Medical Leave Act (FMLA), Americans with Disabilities Act (ADA), and Sick Leave Program (SLP) Process	<p>Management should develop procedures to include processes for coordinating the FMLA, ADA, and SLP programs and a requirement to document all coordination efforts and interactions between the programs.</p> <p>Management should implement and document the results of ongoing monitoring to ensure the programs are effectively coordinated.</p> <p>Management should include language in the "Job Aid for Supervisors - The Interactive Process for ADA" and the "ADA Interactive Process for Successful Accommodation Chart" to provide specific instructions, including a timeframe (i.e., quarterly, bi-annually, annually, etc.) for supervisors to assess the ongoing effectiveness of ADA accommodations provided to their direct reports.</p> <p>Management should implement procedures to instruct supervisors on how to assess ADA accommodations and report the assessments to Employee Relations.</p>
2017-0115	Service Center Audit-Management Memorandum to the Chief of Staff	<p>To strengthen the governance process, all Department-wide policies and procedures should be developed, approved, administered, reviewed, and retained in accordance with the Department's <i>Policy Administration</i> policy.</p>

APPENDIX A

Project #	Audit Name	Recommendation(s)
2017-0115	Service Center Audit- Management Memorandum to the OFM Director	OFM should work with the OWM to publish <i>Department of Revenue Procedures on Managing State-owned Property</i> on the Department procedures intranet site in compliance with the <i>Policy Administration</i> Policy. In addition, OFM should ensure the procedure is communicated to Department staff.
2017-0115	Service Center Audit - Management Memorandum to the ISP Director	Three confidential outstanding corrective actions
2017-0115	Service Center Audit CSP-Orlando	Management should revise walk-in payment processing procedures to include periodic reconciliations of receipts in the receipt books to payments processed through the system. In addition, procedures should include a review of the receipt books to ensure all receipt copies remain intact in the book, voided receipts are clearly marked, receipts are filled out completely, including the employee responsible for taking the payment, and receipts contain no unusual activities or payments.
		Management should revise payment processing procedures for mail-in payments to ensure checks are adequately safeguarded prior to being mailed to the central program office for deposit. This procedure should include keeping the checks in a locked/secure location with access to the key being limited to only a few employees. This change would limit access and assign accountability for the checks to specific employees and keep the checks more secure until mailed.
		Management should implement sign-in logs to document entry into communications rooms on behalf of CSP. In addition, management should ensure restricted area signage is placed on the exterior of communications room doors.
2017-0115	Service Center Audit CSP-Fort Lauderdale	Management should establish written procedures for processing walk-in payments received in the service center. The procedures should include writing receipts for all payments received, reconciling receipts to the payments entered into the database, and reviewing receipt books for completeness and appropriateness. These duties should be performed by different employees within the service center to ensure appropriate segregation of duties.
		Management should ensure employees understand and follow the receipt processing procedures. Additionally, management should periodically review the process to monitor compliance with the procedures.
		The program should ensure employees understand and follow clean desk requirements to ensure confidential information is adequately secured.

APPENDIX A

Project #	Audit Name	Recommendation(s)
2017-0115	Service Center Audit General Tax Administration (GTA) -Orlando	Management should revise payment processing procedures to include audit assessment checks be distributed to the Accountant I for deposit when received. This procedure is consistent with other tax payments received in the service center. A copy of the audit assessment check should be given to the Administrative Assistant for posting.
		Management should also ensure procedures for posting audit assessments payments address preparing payment letters on those occasions when the Administrative Assistant is out of the office and another employee is performing those duties.
		Management should establish a process for securing confidential information within the GTA Orlando Service Center. The process should assign monitoring and oversight responsibilities to an appropriate level of management within the service center and include written procedures for complying with the requirements outlined in the <i>Agency-wide Procedures on Confidential Information</i> . Specifically, the procedures should address the steps required to ensure confidential information is adequately secured at the end of the day.
		Service center management should perform periodic unannounced inspections of work areas and cubicles to identify violations of the information security and secure password policies. Violations identified should be addressed when found.
		Management should work with OFM and DMS to ensure communication room security controls comply with Department policy and Florida Administrative Code.
2017-0115	Service Center Audit GTA-West Palm Beach	Management should revise payment processing procedures to include audit assessment checks be distributed to the Accountant I for deposit when received. This procedure is consistent with other tax payments received in the service center. A copy of the audit assessment check should be given to the Administrative Assistant for posting.
		Management should ensure mobile storage devices are encrypted and appropriately accounted for and safeguarded.
		The process for ensuring confidential information is secured at the end of the day should include procedures for inspecting all documents and folders left on employees' desks. These procedures should be reviewed with all service center supervisors to ensure a thorough review is conducted by whichever supervisor is the last to leave for the day.
		Service center management should perform periodic unannounced inspections of work areas and cubicles to identify violations of the information security and secure password policies. Violations identified should be addressed when found.
		Management should implement an annual reconciliation of all keys and access cards available to those issued. The reconciliation should be signed by the employee performing the reconciliation and reviewed and approved by the service center manager.
2017-0116	Multi-Functional Devices (MFDs)	Eight confidential outstanding corrective actions

APPENDIX B

Summary of Closed Internal Investigations for FY 2017/18

NOTE: These numbers include data from both preliminary reviews and investigations

Disposition	Project #	Investigations Type
Substantiated (12 cases)	14226	Unauthorized Use of State Property, Personnel, and Equipment
	16252	Dishonesty
	16306	Employment Discrimination
	16321	Dual Employment, Outside Employment, Contracts and Business Activities
	16327	Gifts and Gratuities from Outside Sources
	17003	Confidentiality
	17016	Confidentiality
	17021	Falsification of Records
	17068	Confidentiality
	17078	Confidentiality
	17158	Confidentiality
	17229	Confidentiality
Referral (18 cases)	16213	Violation of Law, Rule or Policy
	16277	Violation of Law, Rule or Policy
	17011	Violation of Law, Rule or Policy
	17012	Violation of Law, Rule or Policy
	17026	Violation of Law, Rule, Policy, or Procedure
	17041	Confidentiality
	17075	Discrimination
	17097	Confidentiality
	17120	Stealing and Unauthorized Use of State Property
	17123	Confidentiality
	17134	Violation of Law, Rule, Policy, or Procedure
	17145	Stealing and Unauthorized Use of State Property
	17149	Violation of Law, Rule, Policy, or Procedure
	17154	Stealing and Unauthorized Use of State Property
	17199	Discrimination
	17226	Honesty: Falsification of Records
17244	Confidentiality	
17252	Stealing and Unauthorized Use of State Property	

APPENDIX B

Disposition	Project #	Investigations Type
Unsubstantiated (33 cases)	16209	Theft
	16237	Conduct Unbecoming a Public Employee
	16322	Violation of Law, Rule or Policy
	16331	Violation of Law, Rule or Policy
	17005	Violation of Law, Rule or Policy
	17013	Making a False Statement
	17020	Conflict of Interest: Personal and Financial Relationships and Department of Revenue Duties
	17035	Discrimination
	17048	Violation of Law, Rule, Policy, or Procedure
	17051	Violation of Law, Rule, Policy, or Procedure
	17053	Violation of Law, Rule, Policy, or Procedure
	17070	Conflict of Interest: Personal and Financial Relationships and Department of Revenue Duties
	17079	Violation of Law, Rule, Policy, or Procedure
	17092	Confidentiality
	17101	Confidentiality
	17110	Stealing and Unauthorized Use of State Property: Unauthorized Use of State Property, Personnel, and Equipment
	17114	Violence: Physical Behavior/Violent Touching
	17116	Stealing and Unauthorized Use of State Property
	17128	Confidentiality
	17140	Discrimination
	17146	Violation of Law, Rule, Policy, or Procedure
	17161	Violation of Law, Rule, Policy, or Procedure
	17163	Violation of Law, Rule, Policy, or Procedure
	17175	Falsification of Records
	17188	Confidentiality
	17200	Discrimination
	17213	Discrimination
	17217	Abuse and Destruction of Property
	17231	Honesty: Filing a False Complaint
	17251	Conflict of Interest: Personal and Financial Relationships and Department of Revenue Duties
	17262	Honesty: Falsification of Records
	17263	Conflict of Interest: Personal and Financial Relationships and Department of Revenue Duties
	17305	Confidentiality

Department of Revenue
Office of Inspector General
Annual Report 2017-2018



Report fraud, waste, misconduct, or abuse by calling: (850) 617-8152

Send written complaint information to:

P.O. Box 37372; Tallahassee, Florida 32315-7372

or email: IGReptFraud@FloridaRevenue.com