




Executive  
Director  
Marshall Stranburg

September 25, 2014

**MEMORANDUM**

**TO:** Marshall Stranburg, Executive Director

**FROM:** Sharon Doredant, Inspector General 

**SUBJECT:** Annual Report for Fiscal Year 2013/14

We are pleased to submit the Office of Inspector General's (OIG) Annual Report for the fiscal year ending June 30, 2014. This report is required by section 20.055(7), Florida Statutes, and reflects the major work activities of the Internal Audit, Investigations, and Special Projects Sections.

We are proud of what we do and appreciate the cooperation and support of Revenue management. This office remains committed to enhancing public trust and promoting accountability, integrity, and efficiency in government.

SD/bs0

cc: Strategic Leadership Board  
Office of the Chief Inspector General  
Office of the Auditor General

# Annual Report

FY 2013/14

## FLORIDA Department of Revenue

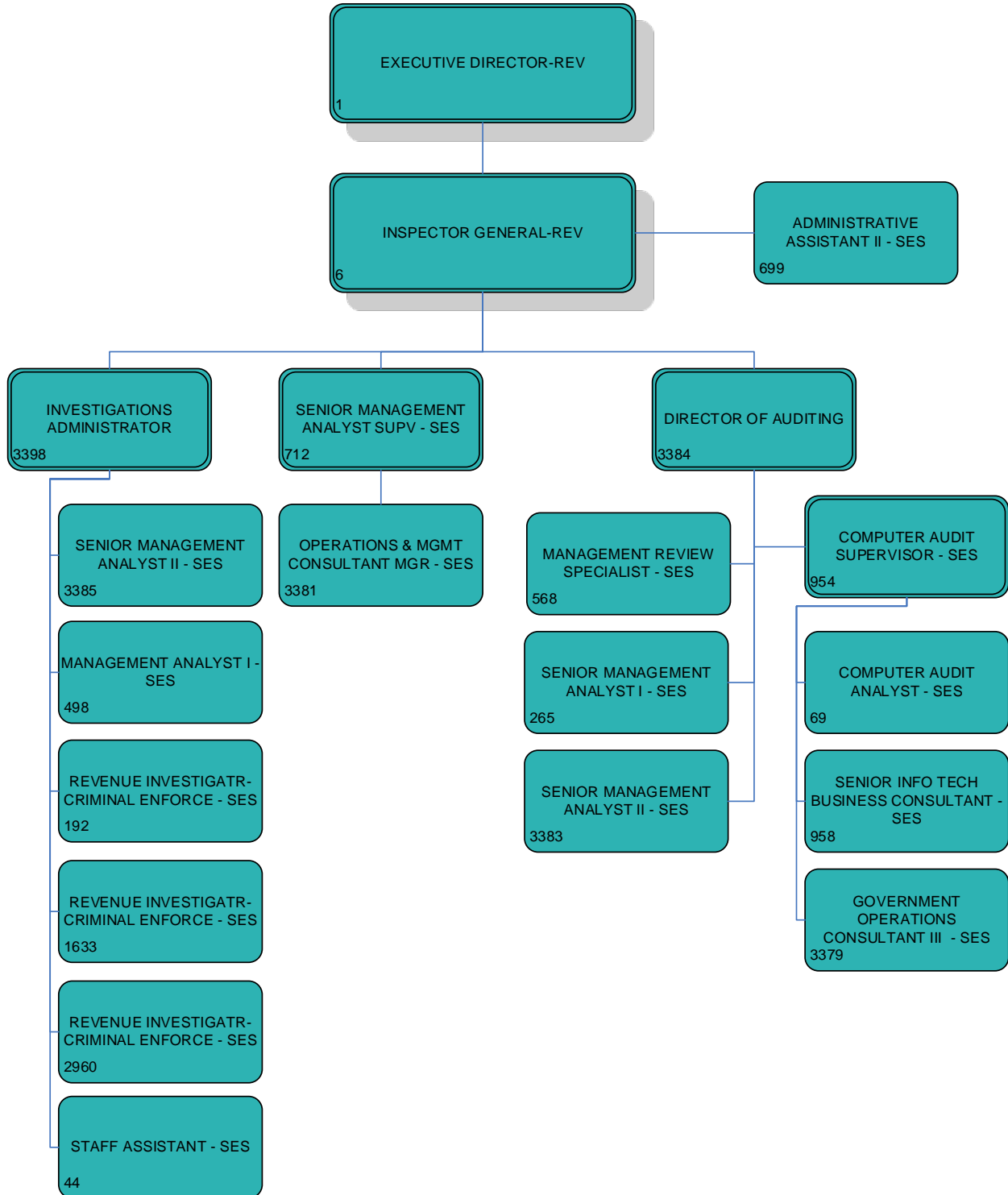
**Office of Inspector General**

*Internal Audits  
Internal Investigations  
Special Projects*

## Table of Contents

Organizational Chart	<a href="#"><u>iii</u></a>
Background	<a href="#"><u>1</u></a>
Internal Audits Section	<a href="#"><u>5</u></a>
Internal Investigations Section	<a href="#"><u>13</u></a>
Special Projects Section	<a href="#"><u>17</u></a>
Appendix A	
Outstanding Corrective Actions for Prior Audit Reports	<a href="#"><u>22</u></a>
Appendix B	
Summary of Closed Internal Investigations for FY 2013/14	<a href="#"><u>30</u></a>

# Office of Inspector General Organizational Chart



## **Background**

An Office of Inspector General (OIG) 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 agency operations. Section 20.055, Florida Statutes, defines the responsibilities of each Inspector General.

### **Annual Report Requirement**

Section 20.055(7), F.S., requires that the OIG submit an annual report to the agency head summarizing its activities during the preceding state 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 each significant recommendation described in previous annual reports on which corrective action has not been completed.
- A summary of each audit and investigation completed during the reporting period.

This document is presented to the Executive Director to comply with the statutory requirements and to provide information on OIG activities as required by Florida law.

### **OIG Responsibilities**

In the Department of Revenue (Revenue), the OIG is responsible for internal audits, internal investigations, and special projects as directed by the Inspector General. These responsibilities are carried out by 19 full-time equivalent positions. The OIG is located 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 Revenue leaders with timely and factual information to improve operations, champion integrity, and ensure the security of Revenue employees and information. They exemplify the best of public service and work hard to accomplish this mission.

As assigned by section 20.055(2), F.S., the duties and responsibilities of the Inspector General include:

- Keeping the Executive Director informed of fraud, abuses, and deficiencies; recommending corrective action; and keeping the Executive Director informed of progress made in corrective action.
- Reviewing actions taken by Revenue to improve program performance and to meet program standards.
- Conducting, supervising, or coordinating audits, investigations, and management reviews relating to the programs and operations of Revenue.
- Conducting, supervising, or coordinating activities to prevent and detect fraud and abuse and to promote economy and efficiency in the administration of Revenue's programs and operations.
- Ensuring effective coordination and cooperation with the Office of the Auditor General (OAG), federal auditors, and other governmental bodies.
- Advising in the development of performance measures, standards, and procedures for the evaluation of department programs.
- Reviewing rules, as appropriate, relating to the programs and operations of Revenue.
- Ensuring that an appropriate balance is maintained between audit, investigative, and other accountability activities.

In addition, the OIG is responsible for conducting financial, compliance, information technology (IT), and performance audits and management reviews relating to the programs and operations of Revenue in accordance with sections 20.055(2)(d) and 20.055(5), F.S.

Additional laws relating to the OIG include:

- Sections 11.51(2) and (3), F.S. – Responses/follow-up for the Office of Program Policy Analysis and Government Accountability (OPPAGA) reports.
- Sections 112.3187–112.31895, F.S. – Responsibility to investigate complaints or information disclosed pursuant to the Whistle-blower's Act.
- Section 282.318(4)(f), F.S. – Audits and evaluations of the security program for data and IT resources.
- Section 215.97, F.S. – The Florida Single Audit Act.
- Section 213.24(2)(b), F.S. – Study of the cost of issuing a bill or refund for any tax listed in section 213.05, F.S.

The Inspector General is required to initiate, conduct, supervise, and coordinate investigations designed to detect, deter, prevent, and remove fraud, waste, mismanagement, misconduct, and other abuses in Revenue. The investigative duties and responsibilities of the Inspector General, pursuant to section 20.055(6), F.S., include:

- Receiving complaints and coordinating all activities required by sections 112.3187–112.31895, F.S., of the Whistle-blower's Act for Revenue.

- Receiving and considering the 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 Revenue's Executive Director regarding investigations conducted, with the exception of whistle-blower investigations, which are reported as required by section 112.3189, F.S.

In addition to the statutory responsibilities assigned by section 20.055, F.S., the OIG's responsibilities include:

- Coordinating Revenue's Workplace Violence Prevention and Response Program.
- Receiving reports from employees who are arrested or charged with a crime, monitoring court actions, and providing management with relevant information upon which to base employment decisions.
- Carrying out other activities to promote economy and efficiency.
- Coordinating Revenue's Fraud Prevention and Response Program.

### **OIG Staff Certifications**

To accomplish the statutorily mandated requirements, technical expertise, and a variety of specialized skills are necessary for creating innovation and expertise within the OIG. OIG employees are certified in a variety of disciplines including: auditing, accounting, crime prevention, information systems, and investigations.

<b>Certifications</b>	<b>Number</b>
Certified Florida Crime Prevention Practitioner – CFCPP	1
Florida Crime Prevention Through Environmental Design Practitioner	1
Certified Law Enforcement	1
Certified Fraud Examiner – CFE	3
Certified Information Systems Auditor – CISA	3
Certified Information Systems Security Professional – CISSP	2
Certified Wireless Security Professional – CWSP	1
Internal Auditor Certification in Information Technology Systems Management According to ISO/IEC 20000-1:2011	2
Certified Internal Auditor – CIA	5
Certified Inspector General – CIG	2
Certified Inspector General Auditor – CIGA	3
Certified Inspector General Investigator – CIGI	5
Six Sigma Yellow Belt Certified	2
Certified Government Auditing Professional	2
Certified Public Accountant – CPA	1

### **Professional Affiliations**

OIG staff members participate in the following professional organizations:

- National Association of Inspectors General
- Tallahassee Chapter of Inspectors General
- Institute of Internal Auditors
- Tallahassee Chapter of the Institute of Internal Auditors
- Tallahassee Chapter of the Association of Government Accountants
- American Institute of Certified Public Accountants
- Florida Institute of Certified Public Accountants
- Association of Certified Fraud Examiners
- Information Systems Audit and Control Association
- FBI Law Enforcement Executive Development Association (LEEDA)
- InfraGard



## Internal Audit Section

In accordance with section 20.055 (5), F.S., the OIG Internal Audit Section (IAS) reviews and evaluates internal controls necessary to ensure Revenue's fiscal accountability. IAS conducts financial, compliance, electronic data processing, and performance audits of the agency and prepares audit reports of the findings. The scope and assignment of audits are determined by the Inspector General; however, the Executive Director may at any time request the Inspector General to perform an audit of a special program, function, or organizational unit. Audits are performed under the direction of the Director of Auditing.

At Revenue, the primary functions of IAS are to conduct independent and objective audits of operations throughout Revenue and to provide consulting engagements for the purpose of improving program operations or processes. IAS staff is committed to identifying and communicating innovative means to improve the way Revenue does business.

IAS performs audits (assurance engagements)<sup>1</sup> and consulting engagements in accordance with the *International Standards for the Professional Practice of Internal Auditing*, published by the Institute of Internal Auditors (IIA), and the *Principles and Standards for Offices of Inspector General (Standards)*, published by the Association of Inspectors General. The *Standards* state, "Internal auditors should review operations and programs to ascertain the extent to which results are consistent with established goals and objectives and to determine whether or not operations and programs are being implemented or performed as intended." As required by *Florida Statutes* and the *Standards*, internal auditors also perform follow-up reviews of corrective action plans in response to the findings of the audits performed by the IAS and external auditors.

According to the *Standards*, internal auditors conduct "assurance" engagements that are an objective examination of evidence to provide an independent assessment on governance, risk management, and control processes for the organization. Internal auditors also conduct "consulting" engagements that are advisory. Consulting engagements 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.

IAS audits provide information regarding the adequacy and effectiveness of Revenue's system of internal controls and quality of performance in carrying out its responsibilities. These engagements include:

---

<sup>1</sup> 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 referencing the *Standards*.

- Reliability and integrity of information.
- Compliance with policies, procedures, laws, and regulations.
- Safeguarding assets.
- Economic and efficient use of resources.
- Assessment of the validity and reliability of performance measures.
- Accomplishment of established objectives and goals for operations or programs.

Audits result in written reports of findings and recommendations and include responses from management. Audit reports are distributed internally to the Executive Director and affected Revenue managers. They are distributed externally to the OAG.

The IAS staff provides a variety of expertise to Revenue through consulting engagements. Many of the consulting engagements involve participation on Revenue teams and performing services at the request of management. Consulting engagements generally do not result in a formal written report; however, they may result in a memorandum or other documentation agreed upon by IAS and management prior to the engagement.

#### **IAS Staff Certifications and Training**

The IAS is comprised of a Computer Audit Analyst, a Senior Information Technology Business Consultant, a Senior Management Analyst I, a Senior Management Analyst II, a Management Review Specialist, a Government Operations Consultant III, a Computer Audit Supervisor, and the Director of Auditing. Professional designations held by staff within the IAS include Certified Information Systems Security Professional, Certified Fraud Examiner, Certified Information Systems Auditor, Certified Public Accountant, Certified Inspector General Auditor, Certified Government Auditing Professional and Certified Internal Auditor.

The *Standards* require audit staff to maintain their professional proficiency through continuing education and training. The staff accomplishes this by attending courses and/or conferences throughout the year. The staff has attended Association of Inspectors General local chapter meetings and training sessions; the Institute of Internal Auditors' webinars as well as local chapter meetings and training sessions; vendor-provided information technology, auditing, and management training; and department-provided employee training.

#### **Annual Risk Assessment and Audit Plan**

Each year, IAS assesses the operations of Revenue to identify areas with the highest levels of risk exposure. Risk is the potential that a chosen action or activity (including the choice of inaction) will lead to a loss (an undesirable outcome). Criteria used for the risk assessment include the complexity of operations, management interest, external oversight, controls, financial materiality, changes in procedures and personnel, results of prior audits, public exposure, auditor judgment, and other criteria as appropriate. Input from executive management, program directors, process owners, and sub-process owners are also considered in the risk assessment.

Using the results of the risk assessment, IAS develops an annual audit plan based on areas with the highest risk exposure. The audit plan includes those areas to be audited or reviewed and the budgeted hours. The audit plan is approved by the Inspector General and the Executive Director and is designed to provide the most effective coverage of Revenue programs and processes while optimizing the use of audit resources.

### **Audit Recommendation Follow-Up**

The *Standards* require auditors to follow up on reported findings and recommendations from previous audits to determine whether management has taken prompt and appropriate corrective action. Every six months, IAS requests status updates from management on the progress of corrective action plans and verifies that corrective actions have resolved the issues on any findings management reported as completed. A report on the status of all findings is provided to executive management, which includes identification of those findings for which the corrective action is past the estimated completion date and an evaluation of the level of risk exposure that the agency may incur if the finding is not corrected.

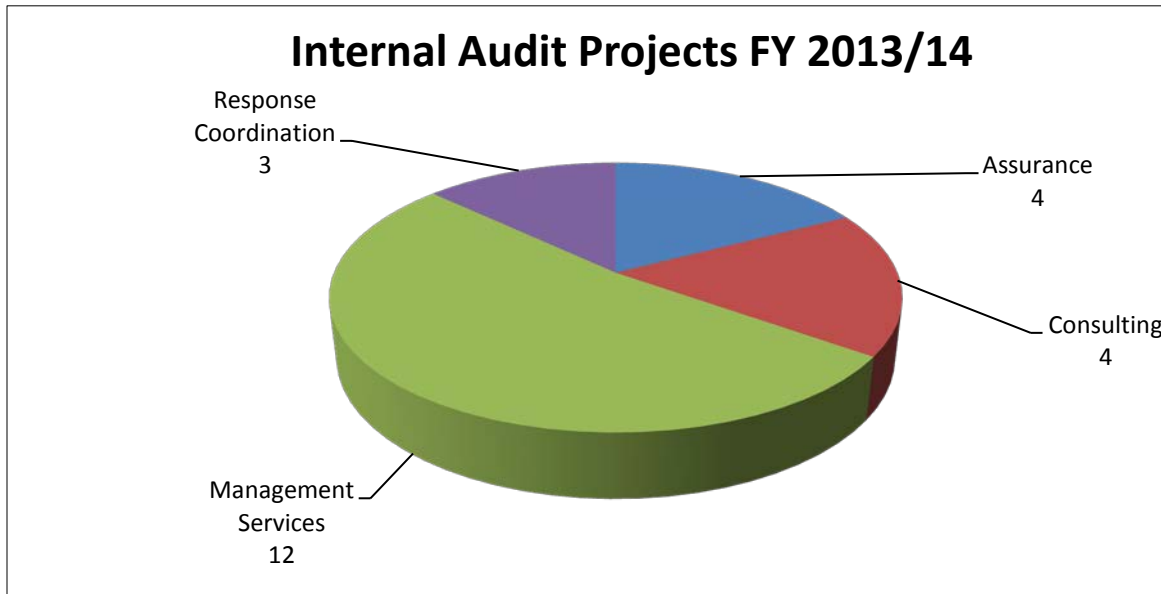
As required by section 20.055(5)(h), F.S., the OIG monitors the accomplishment of Revenue's responses and planned corrective actions to findings and recommendations made in reports issued by the OAG and OPPAGA. The OIG is also required to provide a written report to the Executive Director on the status of planned corrective actions no later than six months after an OAG or OPPAGA report is published. A copy of the report is also provided to the Joint Legislative Auditing Committee. Additionally, as required by section 11.51(3), F.S., the OIG must submit a report no later than 18 months after the release of a report by OPPAGA to provide data and other information describing specifically what Revenue has done to respond to the recommendations contained in the report. The OIG is responsible for coordinating preparation of these status reports and ensuring that they are submitted within the established time frames.

### **Performance Measures**

In accordance with section 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. Additionally, the IAS reviews and verifies the validity and reliability of related performance measures during assurance engagements performed during the year.

## INTERNAL AUDIT PROJECTS

The following chart reflects the number of projects, by project type, completed during FY 2013/14. Detailed descriptions of the projects are included in the following section.



### Audits Conducted During FY 2013/14

During FY 2013/14, the IAS completed four audits. Below is a summary of the reports produced during the year.

#### **Child Support Enforcement (CSE) Payment Data Processing**

The objectives of this audit were to:

- Determine whether CSE contract management exercises adequate control to ensure the secure processing of child support payments and adherence to mandated performance measures.
- Determine whether physical security practices are adequate to ensure the physical security of information resources used to process child support payments.
- Determine whether information security practices in the processing of child support payments comply with federal requirements, *Florida Statutes*, and *Florida Administrative Code*.

The audit concluded:

- Oversight of required performance measures is in place, but some CSE contract management practices could be improved to help ensure secure processing of child support payments.
- The State Disbursement Unit (SDU) has adequate physical security practices in place.

- The SDU contract does not contain language to comply with federal, state, or administrative code requirements for security. However, some general security controls in accordance with best practices are in place to help ensure secure processing of child support payments.

### **Department-Wide Data Security Audit**

The objectives of the audit were to:

- Determine whether selected internal-control activities for protecting IT resources are adequate and consistently implemented.
- Determine whether selected internal-control activities for protecting Revenue's data are adequate and consistently implemented.

Some specific information security issues that are deemed confidential in accordance with section 282.318(4)(f), F.S., were noted during the audit and have been submitted to management in a confidential report.

### **Executive Direction and Support Services Program (EXE) – Office of Workforce Management**

The objectives of the audit were to:

- Determine whether involuntary dismissals of Career Service employees are in compliance with applicable federal and state laws and Revenue's policies and procedures.
- Determine whether employee grievances are in compliance with applicable state laws and Revenue's policies and procedures.
- Determine whether employee files contain all appropriate documentation (official personnel files and Employee Relations files).
- Determine if selection packages are being submitted to Human Resources within 60 days.

The audit concluded:

- Involuntary dismissals of Career Service employees are in compliance with applicable federal and state laws. Documentation of involuntary dismissals of Career Service employees is not in compliance with Revenue's procedures.
- Employee grievances are in compliance with applicable state laws and Revenue's policies and procedures.
- Opportunities exist to improve documentation of employee personnel files.
- While the Office of Workforce Management has improved the process of monitoring selection packages, there is still opportunity for improvement.

### **General Tax Administration Cost Billing Study**

The objectives of the audits were to:

- Determine Revenue's incurred cost to issue a tax bill or delinquency.
- Determine Revenue's incurred cost to issue an automated refund.

The audit concluded:

- Both of the unit costs are below the current \$9.99 threshold; however, an awareness of what these costs represent should be considered. They reflect the initial costs to issue the bills, delinquencies, or automated refunds. With bills and delinquencies in particular, there are likely to be additional downstream collection costs outside the scope of this study that increase total costs to Revenue. In the future, GTA management may wish to analyze these additional costs and explore a higher threshold with respect to bills and delinquencies.

### **Consulting Engagements Conducted During FY 2013/14**

During FY 2013/14, the IAS completed four consulting engagements. Below is a summary of consulting engagements conducted.

#### **Crime Insurance Policy Review**

The purpose was to:

- Determine if participation in the Crime Insurance Policy adequately insures Revenue from losses due to Employee Dishonesty and if continued participation is warranted.
- Determine if participation in the Crime Insurance Policy adequately insures Revenue from losses due to theft, disappearance, or destruction of property and if continued participation is warranted.
- Conduct a risk analysis in order to provide meaningful input into the Department of Management Services' decisions about future coverage opportunities.

#### **IT Voice over Internet Protocol (VOIP) Security**

The purpose was to review security-related issues regarding Revenue's implementation of the VOIP telephone system.

#### **State Disbursement Unit (SDU) Suspense Payment Review**

The purpose was to review SDU suspense payments to identify any questionable disbursements.

## **OCULUS Imaging System**

The purpose was to determine:

- Whether Revenue has adequate controls over the Oculus imaging system to properly manage it.
- Whether Revenue has the ability and resources to maintain the Oculus imaging system.
- Whether adequate information technology controls are in place. This analysis included whether information security, capacity planning, backup and restore, and configuration management are in place.
- Which Revenue program is responsible for support and maintenance of the Oculus imaging system.
- Where the application and images are stored.
- Ownership of document images and meta-data.

## **Other IAS Services**

These services include Follow-Up of Prior Audit Findings, Management Services, and Response Coordination.

IAS assisted the OIG's investigations staff in performing three forensic reviews of computers, by pulling information from Revenue's information systems and providing analyses of data.

IAS staff act as agency coordinators for the Florida Single Audit Act (FSAA). This includes acting as liaisons with program FSAA leads, helping identify legislative effects on Revenue related to the FSAA, and handling inquiries from the public or other state agencies, as well as assisting in the development of Revenue's FSAA Administrative Procedures. IAS is responsible for the annual certification of Revenue's FSAA projects to the Department of Financial Services.

Additionally, IAS staff monitored the programs' corrective action plans to address audit findings and recommendations, coordinated external audits conducted by other entities, and coordinated Revenue's responses to those audits.

Below is a summary of the reports resulting from other IAS services.

### **Follow-Up on Corrective Action Plans as of 6/30/2013**

The purpose was to follow up on the program assertions for the corrective action plans as of June 30, 2013. A summary report was provided to the Executive Director indicating there were 48 open findings, 34 findings verified by OIG staff as closed during the period, and 32 corrective actions overdue.

### **Follow-Up on Corrective Action Plans as of 12/31/13**

The purpose was to follow up on the program assertions for the corrective action plans as of December 31, 2013. A summary report was provided to the Executive Director indicating there were 45 open findings, 15 findings verified by OIG staff as closed during the period, and 29

corrective actions overdue.

**Information Services Program (ISP) ISO 20000 Audit Assistance**

The purpose was to assist ISP with an audit conducted by the International Organization for Standardization (ISO) Foundation resulting in ISO Certification for ISP. ISO 20000 is a set of international standards recognized in the information technology industry.

**Long Range Performance Plan (LRPP) Performance Measures Review FY 2014/15**

The purpose was to assess the reliability and validity of new performance measures submitted for the LRPP.

**Other IAS Accomplishments During FY 2013/14**

In addition to the reports and activities listed above, the IAS accomplished the following during the past fiscal year:

- Assisted the Office of the Chief Inspector General and the IG community by participating on a team to develop enterprise performance measures for internal auditors.
- Assisted the Office of the Chief Inspector General by serving as support to the Citizens Insurance Inspector General Recruitment Committee.
- Assisted the IG community by participating on the committee to produce the Tallahassee Chapter of the Institute of Internal Auditors' quarterly newsletter.
- Assisted the IG community by participating on a team that provided training for beginning auditors.
- Improved internal audit reporting processes within the IAS.
- Provided training to new supervisors within Revenue about the importance of internal controls.

See [Appendix A](#) for a list of the Outstanding Corrective Actions for Prior Audit Reports.



## Internal Investigations Section

The Internal Investigations Section (IIS) is responsible for conducting internal investigations to resolve allegations of violations of Revenue's conduct standards and other policies, rules, directives, and laws impacting Revenue. Investigations may be initiated as a result of information received from Revenue employees, private citizens, taxpayers, other state or federal agencies, or the Whistle-blower's Hotline. The IIS is also responsible for investigating waste and abuse involving Revenue employees, vendors, contractors, or consultants.

The majority of allegations involve violations of Revenue's *Standards of Conduct* such as misconduct, theft, falsification of records, misuse of state property, inappropriate e-mail or Internet transactions, and breaches of confidentiality. These investigations may result in the employee receiving disciplinary action, up to and including dismissal. The IIS also refers information and provides assistance to local, state, and federal law enforcement agencies on cases related to possible criminal violations or activities.

IIS staff conducts a preliminary review of each complaint received by the OIG. The preliminary review process serves to filter complaints to ensure that investigative resources are used effectively and efficiently. Established criteria are used to initially evaluate each complaint to determine the appropriate course of action. When the preliminary review determines that a full investigation is warranted, an investigation is initiated.

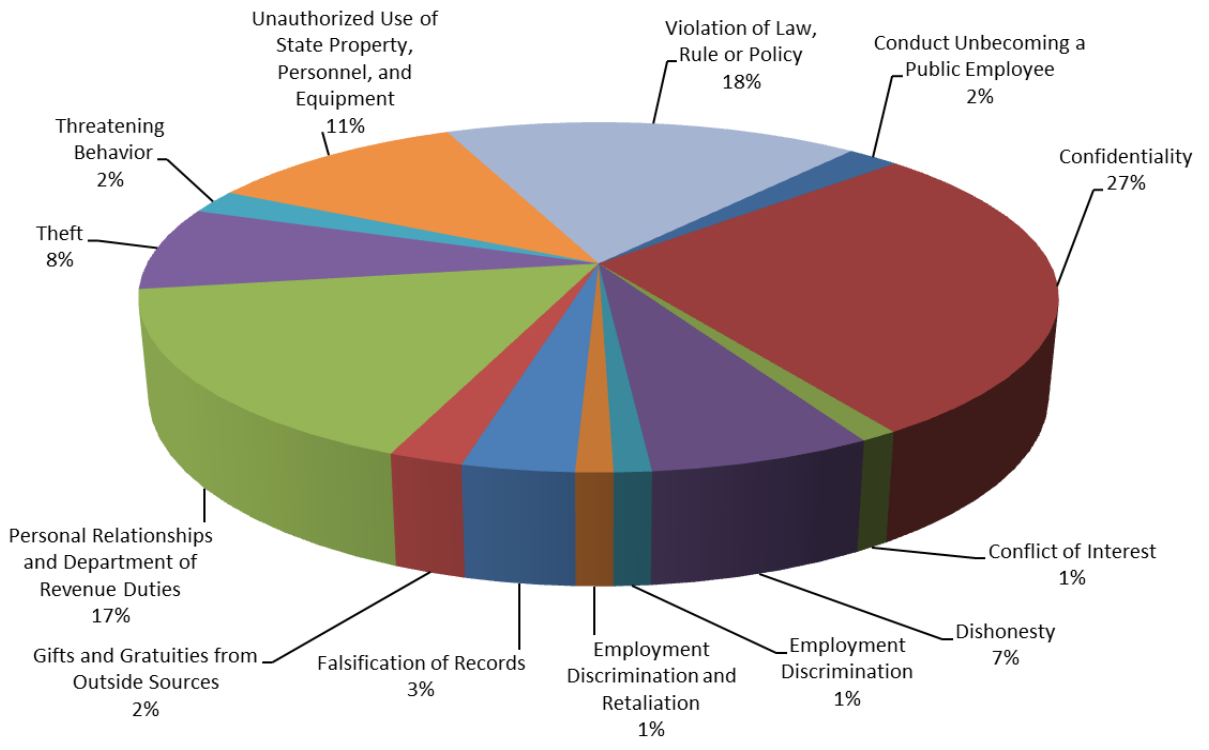
### **Internal Investigations Section (IIS) Accomplishments During FY 2013/14**

- One staff member successfully completed a series of training courses in computer forensics offered by the National White Collar Crime Center (NWC3). These courses provided the staff member with the knowledge and skills needed to perform computer forensics for internal investigations.
- Several staff members attended a 16 hour training course offered by the Association of Certified Fraud Examiners on detecting fraud.
- Held periodic meetings with the accreditation manager to ensure *IIS Policies and Procedures Manual* is current and in compliance with the Commission for Florida Law Enforcement Accreditation (CFA) standards.
- Significantly reduced travel costs for investigations by conducting investigatory interviews, when appropriate, remotely through a secured Internet video conferencing system.

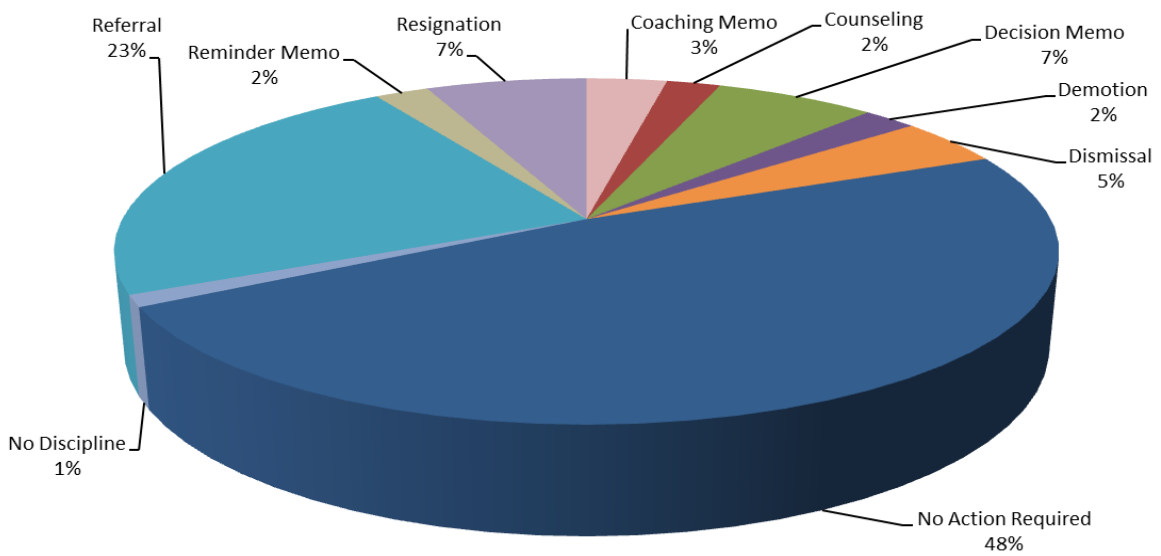
IIS completed 35 investigations and 56 preliminary reviews during FY 2013/14.

The following charts reflect the types and outcomes of cases closed, including both preliminary reviews and investigations, during FY 2013/14.

### Cases Closed by Type



### Final Disposition of Closed Cases



### **Investigation Summaries for FY 2013/14**

A number of significant cases were conducted during FY 2013/14. The following are highlights of some of these cases:

#### **Employment Discrimination-Sexual Harassment**

The OIG received information from the Discrimination Intake Officer that an employee may have subjected another employee to unwelcome and offensive physical behavior of a sexual nature on several occasions. The OIG's investigation revealed sufficient evidence that the employee violated Revenue's Non-Discrimination Policy and Complaint Procedures by engaging in inappropriate behavior of a sexual nature in the workplace, as well as, interfered with the investigation by being uncooperative for failing to answer questions completely, accurately, and truthfully. The employee retired from Revenue.

#### **Confidentiality**

The OIG received information from management that an employee may have accessed and viewed confidential information for nonbusiness-related purposes. The employee admitted to accessing and viewing confidential information as well as disclosing the information to a relative. The investigation also determined the employee was dishonest when not admitting to disclosing confidential driver's license information to the relative. The employee resigned from Revenue.

#### **Dishonesty**

The OIG received a complaint from management that an employee allegedly forged a supervisor's signature on two documents without the supervisor's knowledge, sent the forged/falsified documents to an external partner, and falsified a note to conceal his error in an information system used by Revenue. The OIG investigation substantiated the allegation and the employee was dismissed.

#### **Unauthorized Use of State Property**

The OIG received information from the Discrimination Intake Officer that a supervisor found documents on a shared office printer that contained personal texting conversations between two individuals; one was later identified as a Revenue employee. The OIG investigation found that the employee used her Revenue computer and printer without authorization to print several pages of personal documents containing profane language and threatening comments; accessed, viewed, and disclosed confidential information; and connected a personal flash drive to a Revenue computer to download information from the Internet and to edit, save, or print personal documents. The employee was dismissed.

**Theft**

The OIG investigated an allegation of theft by a contractor's employee. After researching the allegations, it was determined that the contract employee colluded with a customer to divert funds. The OIG referred the issue to the Florida Department of Law Enforcement (FDLE). The customer and contractor's employee were later arrested for theft.

**Falsification of Records**

The OIG received allegations from management that an employee may be recording hours worked on her People First and internal timesheets for work she did not perform while teleworking. The OIG investigation revealed that the employee falsified her People First and internal timesheet for one month and was also negligent in recording time worked in several other months. Additionally, the OIG found that the employee failed to obtain prior approval from her supervisor for leave taken. The employee resigned in lieu of termination.

See [Appendix B](#) for a Summary of Closed Cases for FY 2013/14, including data from both preliminary reviews and investigations.

## Special Projects Section

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 new and revised agency policies.

The goals of the SPS are to provide a work environment for Revenue employees free from fear of violence and to provide management with information necessary to ensure a desired level of integrity among Revenue staff.

### **Special Projects Section Accomplishments During FY 2013/14**

- Coordinated revision of the agency's Workplace Violence Prevention and Response Procedures to provide specific guidance on working with irate customers and customers who have previously been identified as a Potentially Dangerous Contact (PDC).
- Began implementation of a fraud program for Revenue, including presentation of a proposed agency-wide policy specifically addressing fraud prevention and response for approval by the Strategic Leadership Board (SLB).

### **Workplace Violence**

Revenue's security 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. Revenue'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 aware of the incident and makes recommendations for appropriate action.

Workplace violence can originate from internal or external sources. Most reported workplace violence incidents originate from external sources. External workplace violence incidents include assaults and threats made by customers against Revenue employees as a result of their official duties. More serious threats are reported to law enforcement for assistance in threat assessment and determination of appropriate response.

External sources of workplace violence also include threats made to Revenue by a customer but directed toward someone else, such as a noncustodial parent in a child support case threatening to harm the custodial parent or child in the case. The *Workplace Violence Prevention and*

*Response Policy* requires that Revenue staff notify local law enforcement of the threat and also attempt to notify the person who the threat was directed toward so he/she can determine the most appropriate action to provide for his/her safety.

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

Threats of suicide made by customers to Revenue employees are also reported to and logged by the SPS as external sources 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 operating programs of Revenue. This indicator flag serves as notice to an employee that a PDC is associated with the case and 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 our statutory tax administration or child support enforcement responsibilities are carried out in relation to a PDC account.

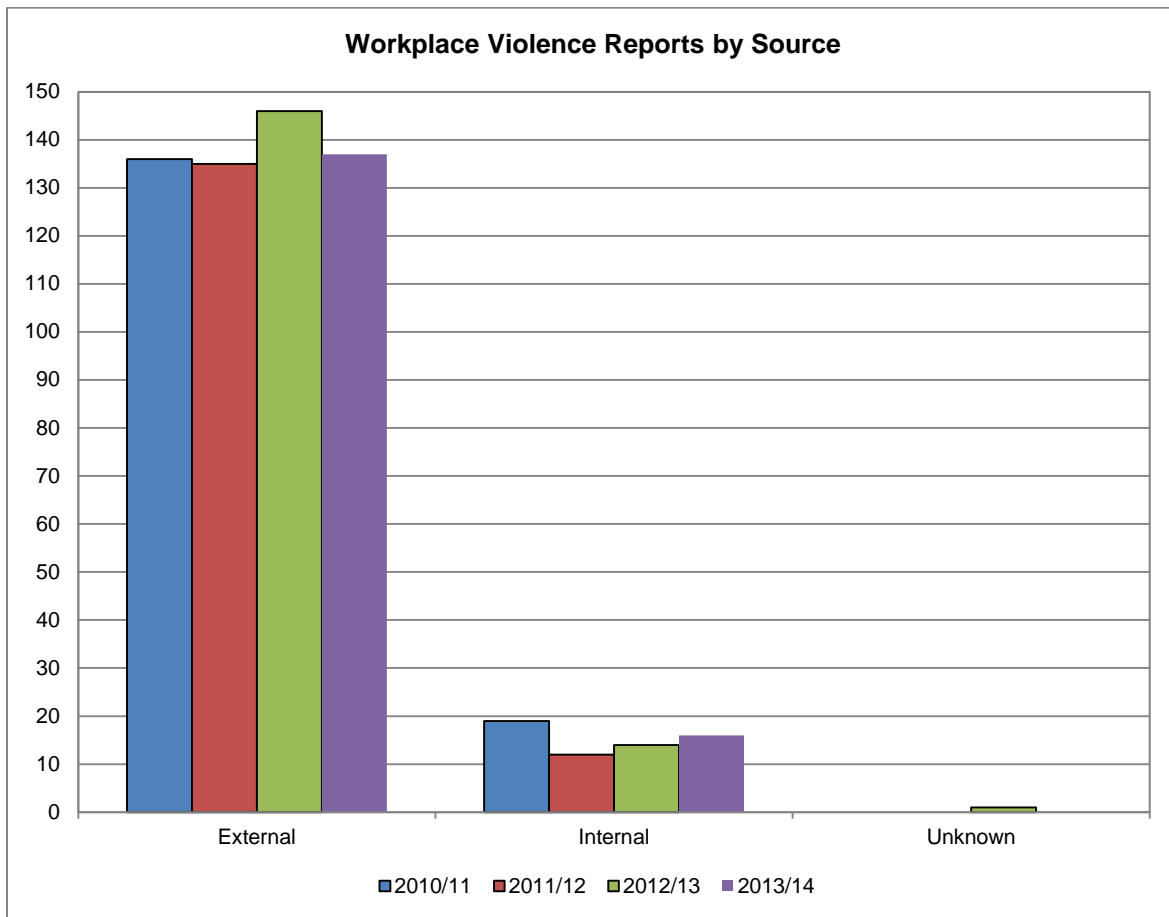
During this fiscal year, SPS staff coordinated the development and approval of procedures to provide staff and management with guidelines on dealing with an irate customer and how to work with a customer who has previously been identified as a PDC. The new procedures provide guidance on how to react to an irate customer exhibiting a variety of specific behaviors to defuse the situation. The procedures address how to obtain approval to restrict contact with a customer and the issuance of trespass warnings.

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 Revenue's Workplace Violence Response Team (WPV Team). The WPV Team consists of the Inspector General, the OIG Special Projects Manager, the Employee Relations Manager, and the Chief Assistant General Counsel for the EXE Program. The WPV Team works cooperatively to determine and advise management of the best response to reported incidents. The WPV Team's recommendation(s) to management may include disciplinary action, counseling, mitigation, or referral to Revenue's Employee Assistance Program (EAP). The WPV Team may also request an internal investigation if facts of the incident cannot be determined.

Domestic violence affecting the workplace is a primary concern for any agency or business. Domestic violence can be initiated by an external or internal source. Revenue's *Standards of Conduct* require any employee who is named as the respondent in an injunction for protection

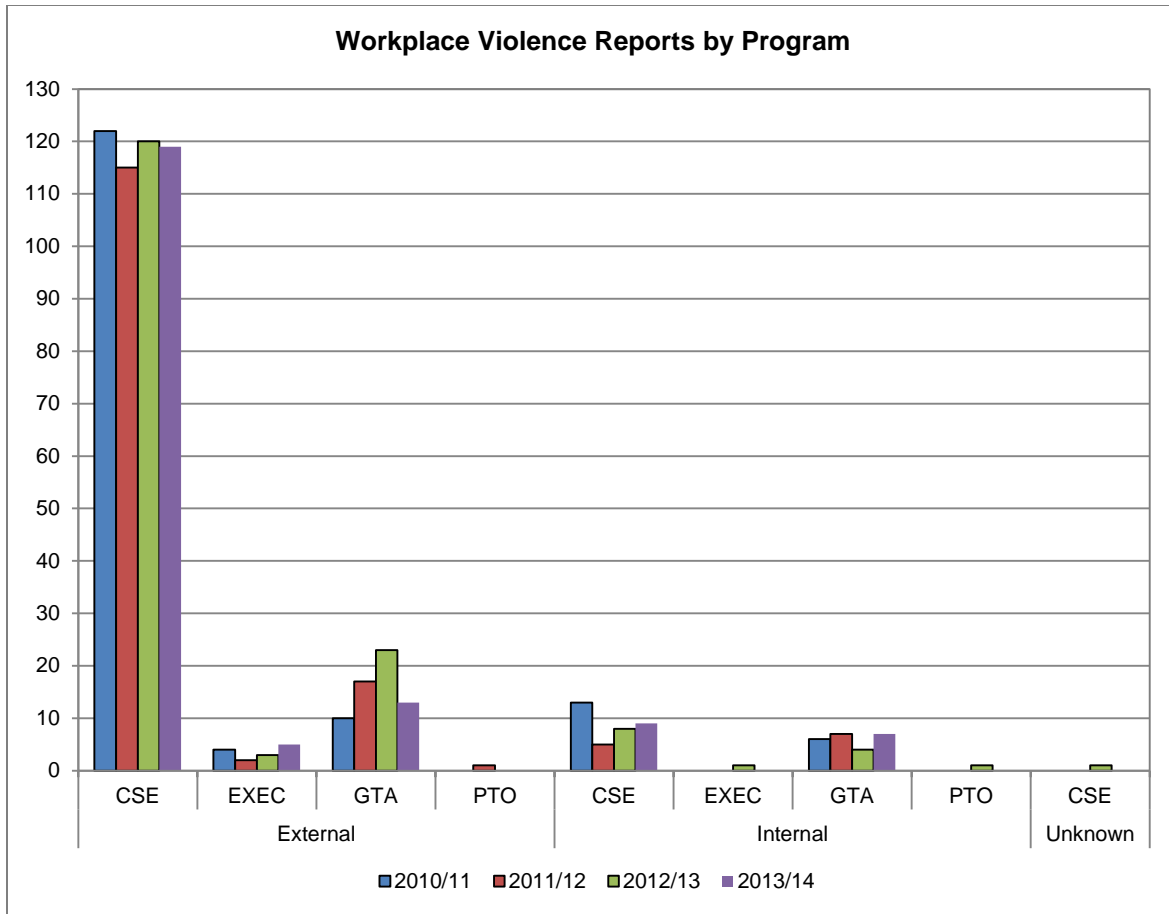
against domestic violence, or any similar injunction, to report the injunction to the OIG. The agency's *Workplace Violence Prevention and Response Policy* encourages employees to report if they are the petitioner in an injunction for protection against domestic violence and if they have any concern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

The following chart reflects the total number of workplace violence incident reports received for the past four years by source.



A total of 153 reports of workplace violence were received during FY 2013/14, a slight decrease from the 161 incidents reported during the previous fiscal year. Sixteen of these incidents involved a Revenue employee as the perpetrator.

The following chart reflects the number of workplace violence incidents received for the past four years by source for each program.



During FY 2013/14, CSE reported 119 incidents from external sources and 9 incidents from internal sources, GTA reported 13 incidents from external sources and 7 incidents from internal sources, EXE reported 5 incidents from external sources, and no incidents were reported from the Property Tax Oversight Program (PTO) or ISP during the fiscal year.

The SPS continually seeks methods and strategies to combat workplace violence and apply them in our day-to-day activities.

**Employee Arrest Reports**

The SPS is responsible for receiving and following up on reports of current employees who are arrested or charged with criminal offenses. Revenue’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 60 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 60 days imprisonment and/or more than a \$500 fine.
- The resolution of any outstanding arrest warrant.



- Being named as the respondent in an Injunction for Protection against Domestic Violence, or any similar injunction.

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. The SPS will also open a review file to monitor court actions and ensure the employee meets all of the reporting requirements established in Revenue'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 the 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.

Twenty-seven current arrest reports were received and twenty-two current arrest follow-up review cases were closed during the fiscal year.

Nineteen current arrest follow-up review cases were pending outcome at the close of the fiscal year.

### **Fraud Program**

SPS staff worked throughout the year to develop and establish a fraud prevention and response program for Revenue. The first step was to draft and champion an agency-wide fraud prevention and response policy to:

- Demonstrate Revenue's commitment to combatting fraud and corruption.
- Communicate management's commitment to securing Revenue's assets and maintaining the highest possible ethical standards.
- Provide clear guidance to management and employees on action to take if they suspect fraudulent activity within or affecting Revenue services.

Revenue's SLB approved the *Fraud Prevention and Response Policy* during their July 17, 2014, meeting and established a September 1, 2014, effective date. In anticipation of the roll-out of the new policy, during FY 2013/14, SPS staff:

- Created a high-level Fraud Awareness training module for managers and supervisors and made fraud awareness presentations to various groups. Seven fraud awareness presentations were made during the fiscal year.
- Participated in the Internal Audit Section's annual risk assessment. A fraud risk category was added to the risk tabulation for each of Revenue's business processes and fraud risk was specifically discussed with and considered by managers participating in the audit risk assessment process.

## Appendix A

### Outstanding Corrective Actions for Prior Audit Reports

IAS Engagements Outstanding Corrective Actions as of 6/30/14		
Project No.	Audit Name	Recommendation
2007-0067	Internet Tax Applications	Confidential
2007-0067	Internet Tax Applications	Confidential
2008-0115-A	ISP Security Monitoring and Response	1. We recommend ISMCP policies and procedures be periodically reviewed as stated in the ISP Policy Development and Maintenance Manual.
2008-0115-A	ISP Security Monitoring and Response	4. We recommend ISP management follow the established industry standards, <i>Florida Administrative Code</i> , and Revenue's policies and procedures for audit trails to include developing adequate written policy and procedures to ensure audit trails are collected and secured.
2009-0101	Service Support Change	6. We recommend that ISP management enforce the Change Master Policy requirement that the Change Manager be notified of the "successful or unsuccessful completion of all changes within 24 hours of the scheduled implementation of the change."
2009-0107 A	Contract Management Process	1.2 We recommend the Purchasing and Contract Management Manual include specific procedures and requirements, such as those noted above and others as required, to ensure Revenue's activities for the monitoring of contracts are consistently conducted and meet expectations and objectives.
2009-0107 A	Contract Management Process	1.3 We recommend the Purchasing management staff work with the Office of Communication and Professional Development staff to develop best practices contract monitoring training, deploy this training to contract managers, and require contract managers to complete periodic ongoing training to maintain an acceptable level of competence and skill.
2009-0107 A	Contract Management Process	1.4 We also recommend the contract manager's supervisors complete the contract monitoring training.

IAS Engagements Outstanding Corrective Actions as of 6/30/14		
Project No.	Audit Name	Recommendation
2009-0107 A	Contract Management Process	3. We recommend Purchasing Process management require contract managers to enter the necessary information in the Contract Accountability and Tracking System to ensure the system is capturing complete and accurate data.
2009-0107 A	Contract Management Process	4. We recommend program management develop performance measures and standards for the Contract Management Process and monitor performance against those standards.
2009-0113-A	ISP/Agency Application Management-Requirements	1. We recommend ISP request assistance through Revenue's SLB in gaining program participation and representation in the Requirements Process.
2009-0113-A	ISP/Agency Application Management-Requirements	2. We recommend ISP management in conjunction with program management develop a requirements methodology that will ensure that business requirements are adequately and consistently defined by the customer and documented to support their overall business objectives. We also recommend ISP, GTA, PTO and EXE develop a software requirements specification template to be incorporated into the requirements methodology as part of the Information Systems Design Methodology (ISDM).
2009-0113-A	ISP/Agency Application Management-Requirements	3. We recommend ISP implement performance measures to determine the efficiency and effectiveness of the Applications Management – Requirements Business Process for all development projects.
2009-0116 A	GTA Cash Handling	2.2 We recommend GTA management consider adopting a centralized collection system that does not accept payments at the local offices or, at a minimum, discontinue the acceptance of cash (currency) payments at the GTA service centers.

<b>IAS Engagements Outstanding Corrective Actions as of 6/30/14</b>		
<b>Project No.</b>	<b>Audit Name</b>	<b>Recommendation</b>
2010-0110	General Tax Administration Receivables Write-Offs (DL-17)	3.1 We recommend GTA management write off uncollectible receivables in accordance with Revenue's Procedure for Identifying and Writing-Off Non-Collectible Receivables. Additionally, we suggest that GTA management pursue SAP system changes to establish flags and date identification for those accounts that should be retained in an active status, such as litigation and audit, so that the write-off procedures can be performed without manual intervention.
2010-0110	General Tax Administration Receivables Write-Offs (DL-17)	3.2 We recommend that Revenue accrue and prepare an allowance for all types of taxes collected by Revenue, with the exception of unemployment tax (now reemployment tax), which is recorded by the Agency for Workforce Innovation (now called the Department of Economic Opportunity).
2010-0113 A	Contract Compliance and Management – CSE DNA Contract	1. We recommend CSE independently verify the vendor's performance for the average test result turnaround time to ensure that the vendor is meeting this measure.
2010-0115-A	ISP Telecom VOIP	1.1 Confidential
2010-0115-A	ISP Telecom VOIP	1.2 Confidential
2010-0115-A	ISP Telecom VOIP	1.4 Confidential
2010-0115-A	ISP Telecom VOIP	2.1 Confidential
2010-0115-A	ISP Telecom VOIP	2.2 Confidential
2010-0115-A	ISP Telecom VOIP	2.3 Confidential
2010-0115-A	ISP Telecom VOIP	2.4 Confidential
2010-0115-A	ISP Telecom VOIP	2.5 Confidential
2010-0115-A	ISP Telecom VOIP	2.6 Confidential
2010-0115-A	ISP Telecom VOIP	2.7 (a) Confidential
2010-0115-A	ISP Telecom VOIP	2.9 (a) Confidential
2010-0115-A	ISP Telecom VOIP	2.9 (b) Confidential
2010-0119-A2	GTA Dallas Out-Of-State Service Center – Confidential	1.1 Confidential
2010-0119-A2	GTA Dallas Out-Of-State Service Center – Confidential	1.2 Confidential

<b>IAS Engagements Outstanding Corrective Actions as of 6/30/14</b>		
<b>Project No.</b>	<b>Audit Name</b>	<b>Recommendation</b>
2010-0119-A2	GTA Dallas Out-Of-State Service Center – Confidential	2.6 Confidential
2010-0120-A2	GTA Pittsburgh Out-Of-State Service Center – Confidential	1.2 Confidential
2010-0120-A2	GTA Pittsburgh Out-Of-State Service Center – Confidential	2.5 Confidential
2010-0121-A2	GTA In-State Service Centers – Miami, Coral Springs, West Palm Beach-Confidential	1.2 Miami North Confidential
2010-0121-A2	GTA In-State Service Centers – Miami, Coral Springs, West Palm Beach – Confidential	1.2 West Palm Beach Confidential
2010-0121-A2	GTA In-State Service Centers – Miami, Coral Springs, West Palm Beach – Confidential	1.4 Miami North Confidential
2010-0121-A2	GTA In-State Service Centers – Miami, Coral Springs, West Palm Beach – Confidential	1.4 Miami South Confidential
2010-0121-A2	GTA In-State Service Centers – Miami, Coral Springs, West Palm Beach – Confidential	1.4 West Palm Beach Confidential
2010-0121-A2	GTA In-State Service Centers – Miami, Coral Springs, West Palm Beach – Confidential	2.5 Miami Confidential
2011-0105-A	ISP Service Delivery Continuity Process	1.1 Confidential
2011-0105-A	ISP Service Delivery Continuity Process	1.2 Confidential

IAS Engagements Outstanding Corrective Actions as of 6/30/14		
Project No.	Audit Name	Recommendation
2011-0105-A	ISP Service Delivery Continuity Process	1.3 Confidential
2011-0105-A	ISP Service Delivery Continuity Process	1.7 Confidential
2011-0106-A1	CSE Payment Processing – Fund Distribution	1. The Department should consider reconciling the daily disbursement instruction file sent to the SDU with the actual bank disbursement records for each disbursement.
2011-0117-A2	GTA Return and Revenue Processing – Building L	1.1 We recommend Building L management implement or enforce existing procedures to improve internal controls for ensuring physical security.
2011-0117-A2	GTA Return and Revenue Processing – Building L	1.2 We recommend Building L management implement or enforce existing procedures to improve internal controls for improving emergency management.
2011-0130-A	ISP Network Infrastructure Deployment Process	2.1 Confidential
2011-0130-A	ISP Network Infrastructure Deployment Process	2.3 Confidential
2011-0130-A	ISP Network Infrastructure Deployment Process	3.1 Confidential
2011-0134-A2	CSE, GTA, PTO Tampa Service Centers – Confidential	1.1 Confidential
2012-0115	Department-Wide Data Security	1(b).1 Confidential
2012-0115	Department-Wide Data Security	1(b).2 Confidential
2012-0115	Department-Wide Data Security	1(c) Confidential
2012-0115	Department-Wide Data Security	1(d) Confidential
2012-0115	Department-Wide Data Security	1(e) Confidential

IAS Engagements Outstanding Corrective Actions as of 6/30/14		
Project No.	Audit Name	Recommendation
2012-0115	Department-Wide Data Security	2(a) Confidential
2012-0115	Department-Wide Data Security	2(b) Confidential
2012-0115	Department-Wide Data Security	2(d) Confidential
2012-0116	CSE Payment Data Processing Audit	1.1 We recommend CSE contract managers designate which SDU employees require a criminal background check and enforce the contract provision requiring criminal background checks.
2012-0116	CSE Payment Data Processing Audit	1.2 We also recommend that CSE management ensure that data processing contracts require vendors to have SOC 2, Type 2, attestation engagements performed at all locations where information processing is performed.
2012-0116	CSE Payment Data Processing Audit	3.1 We recommend that future contracts contain the specific requirement that information security is compliant with Rule 71A-1, Florida Administrative Code.
2012-0120	EXE Workforce Management	1.1 Procedures should provide supervisors specific guidance related to deadlines for submitting documents and how to handle situations when an employee is not available to participate in the separation process.
2012-0120	EXE Workforce Management	1.2 Operating procedures should include requirements for the Office of Workforce Management (OWM) to monitor receipt of documents detailed in Department Procedure Number DOR-1080-032C.
2012-0120	EXE Workforce Management	1.3 For efficiency purposes, OWM should consider incorporating the items included in the "Notice of Separation" form into the phone book step used to remove access. The "Notice of Separation" form could be eliminated from the process.

IAS Engagements Outstanding Corrective Actions as of 6/30/14		
Project No.	Audit Name	Recommendation
2012-0120	EXE Workforce Management	<p>3.1 Operating procedures related to Department Policy Number DOR-1080-30B should include the following requirements for OWM staff:</p> <ul style="list-style-type: none"> <li>• Monitor receipt of documents.</li> <li>• Reminders to managers of hiring supervisors when submissions are late or not received.</li> </ul>
2012-0120	EXE Workforce Management	<p>3.2 OWM should review quality assurance practices to ensure all documents received are entered into Oculus.</p>
2012-0120	EXE Workforce Management	<p>3.3 For added confidentiality, best practices suggest segregating I-9 Forms from other personnel records. Segregating the forms will limit unnecessary access to citizenship, national origin, race, and other protected information. Additionally, in the event it receives notice of an I-9 audit, OWM will be able to quickly produce the I-9 Forms without searching through personnel files. Best practices also suggest if I-9 verification documents (Social Security Card and Driver's License) are photocopied, to include them with the form.</p>
2012-0120	EXE Workforce Management	<p>4.1 Controls should be put in place to ensure Settlement Agreements are submitted by the Office of General Counsel to OWM for inclusion in employee files.</p>
2012-0120	EXE Workforce Management	<p>5.1 While the new procedures have increased the submission rates, we recommend the following enhancements.</p> <p>The Standard Operating Procedure for selection packages can be improved by adding:</p> <ul style="list-style-type: none"> <li>• A specific time frame for Human Resources to notify next level of management when packages are not received after multiple reminders.</li> <li>• Instructions for special circumstances, such as appointments or multiple hires for the same package.</li> </ul>



<b>IAS Engagements</b> <b>Outstanding Corrective Actions as of 6/30/14</b>		
<b>Project No.</b>	<b>Audit Name</b>	<b>Recommendation</b>
2012-0120	EXE Workforce Management	5.2 The new tracking database can be improved by adding a date for escalating a notice to upper management if the package is not received and by adding the following indicators: <ul style="list-style-type: none"> <li>• Partial submissions.</li> <li>• Multiple positions filled from the same package.</li> <li>• Appointments.</li> </ul>

## Appendix B

### Summary of Closed Internal Investigations for FY 2013/14

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

Project Number	Disposition	Type
12092	Substantiated	Falsification of Records
12128	Unsubstantiated	Confidentiality
12195	Substantiated	Confidentiality
12203	Substantiated	Confidentiality
12223	Unsubstantiated	Unauthorized Use of State Property, Personnel, and Equipment
12234	Referral	Violation of Law, Rule, or Policy
12244	Unsubstantiated	Personal Relationships and Department of Revenue Duties
12265	Substantiated	Confidentiality
12277	Unsubstantiated	Confidentiality
12282	Unsubstantiated	Violation of Law, Rule, or Policy
12292	Substantiated	Conflict of Interest
12295	Referral	Confidentiality
12303	Substantiated	Confidentiality
12304	Referral	Theft
12308	Unsubstantiated	Employment Discrimination and Retaliation
12311	Substantiated	Employment Discrimination
12319	Referral	Confidentiality
12324	Referral	Violation of Law, Rule, or Policy
12328	Referral	Falsification of Records
12329	Unsubstantiated	Threatening Behavior
12330	Unsubstantiated	Conduct Unbecoming a Public Employee
12332	Substantiated	Confidentiality
13001	Unsubstantiated	Dishonesty
13002	Unsubstantiated	Confidentiality
13003	Substantiated	Personal Relationships and Department of Revenue Duties
13004	Referral	Theft
13005	Substantiated	Personal Relationships and Department of Revenue Duties
13006	Unsubstantiated	Violation of Law, Rule, or Policy
13009	Unsubstantiated	Unauthorized Use of State Property, Personnel, and Equipment
13011	Unsubstantiated	Confidentiality
13013	Unsubstantiated	Personal Relationships and Department of Revenue Duties
13014	Referral	Confidentiality
13015	Substantiated	Confidentiality
13020	Unsubstantiated	Violation of Law, Rule, or Policy

Project Number	Disposition	Type
13022	Unsubstantiated	Confidentiality
13028	Substantiated	Dishonesty
13029	Substantiated	Confidentiality
13032	Substantiated	Confidentiality
13033	Unsubstantiated	Confidentiality
13039	Unsubstantiated	Confidentiality
13042	Unsubstantiated	Theft
13049	Unsubstantiated	Conduct Unbecoming a Public Employee
13050	Unsubstantiated	Unauthorized Use of State Property, Personnel, and Equipment
13053	Unsubstantiated	Confidentiality
13055	Unsubstantiated	Personal Relationships and Department of Revenue Duties
13056	Substantiated	Falsification of Records
13057	Referral	Unauthorized Use of State Property, Personnel, and Equipment
13058	Substantiated	Personal Relationships and Department of Revenue Duties
13060	Unsubstantiated	Violation of Law, Rule, or Policy
13064	Substantiated	Personal Relationships and Department of Revenue Duties
13065	Unsubstantiated	Confidentiality
13070	Unsubstantiated	Confidentiality
13071	Substantiated	Confidentiality
13087	Substantiated	Confidentiality
13094	Substantiated	Personal Relationships and Department of Revenue Duties
13096	Unsubstantiated	Personal Relationships and Department of Revenue Duties
13104	Unsubstantiated	Dishonesty
13105	Unsubstantiated	Dishonesty
13107	Unsubstantiated	Personal Relationships and Department of Revenue Duties
13110	Unsubstantiated	Gifts and Gratuities from Outside Sources
13114	Unsubstantiated	Dishonesty
13115	Substantiated	Confidentiality
13120	Substantiated	Unauthorized Use of State Property, Personnel, and Equipment
13123	Unsubstantiated	Violation of Law, Rule, or Policy
13128	Referral	Violation of Law, Rule, or Policy
13129	Referral	Personal Relationships and Department of Revenue Duties
13130	Unsubstantiated	Dishonesty
13137	Unsubstantiated	Violation of Law, Rule, or Policy
13146	Unsubstantiated	Theft
13147	Unsubstantiated	Unauthorized Use of State Property, Personnel, and Equipment
13151	Unsubstantiated	Personal Relationships and Department of Revenue Duties
13152	Unsubstantiated	Personal Relationships and Department of Revenue Duties
13157	Referral	Violation of Law, Rule, or Policy

Project Number	Disposition	Type
13161	Unsubstantiated	Theft
13163	Unsubstantiated	Personal Relationships and Department of Revenue Duties
13168	Unsubstantiated	Violation of Law, Rule, or Policy
13170	Unsubstantiated	Threatening Behavior
13172	Substantiated	Theft
13173	Referral	Violation of Law, Rule, or Policy
13176	Referral	Theft
13180	Unsubstantiated	Violation of Law, Rule, or Policy
13182	Referral	Violation of Law, Rule, or Policy
13187	Referral	Violation of Law, Rule, or Policy
13189	Referral	Personal Relationships and Department of Revenue Duties
13191	Referral	Confidentiality
13195	Referral	Gifts and Gratuities from Outside Sources
13208	Referral	Violation of Law, Rule, or Policy
13219	Referral	Unauthorized Use of State Property, Personnel, and Equipment
13220	Substantiated	Unauthorized Use of State Property, Personnel, and Equipment
13238	Unsubstantiated	Unauthorized Use of State Property, Personnel, and Equipment
13258	Substantiated	Unauthorized Use of State Property, Personnel, and Equipment