FLORIDA
Executive
Director
Marshall Stranburg

September 10, 2015

TO: Marshall Stranburg, Executive Director

FROM: Sharon Doredant, Inspector General

SUBJECT: Annual Report for Fiscal Year 2014/15

We are pleased to submit the Office of Inspector General's (OIG) Annual Report for the fiscal year ending June 30, 2015. This report is required by section 20.055(8), 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/bso

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

FLORIDA DEPARTMENT OF REVENUE

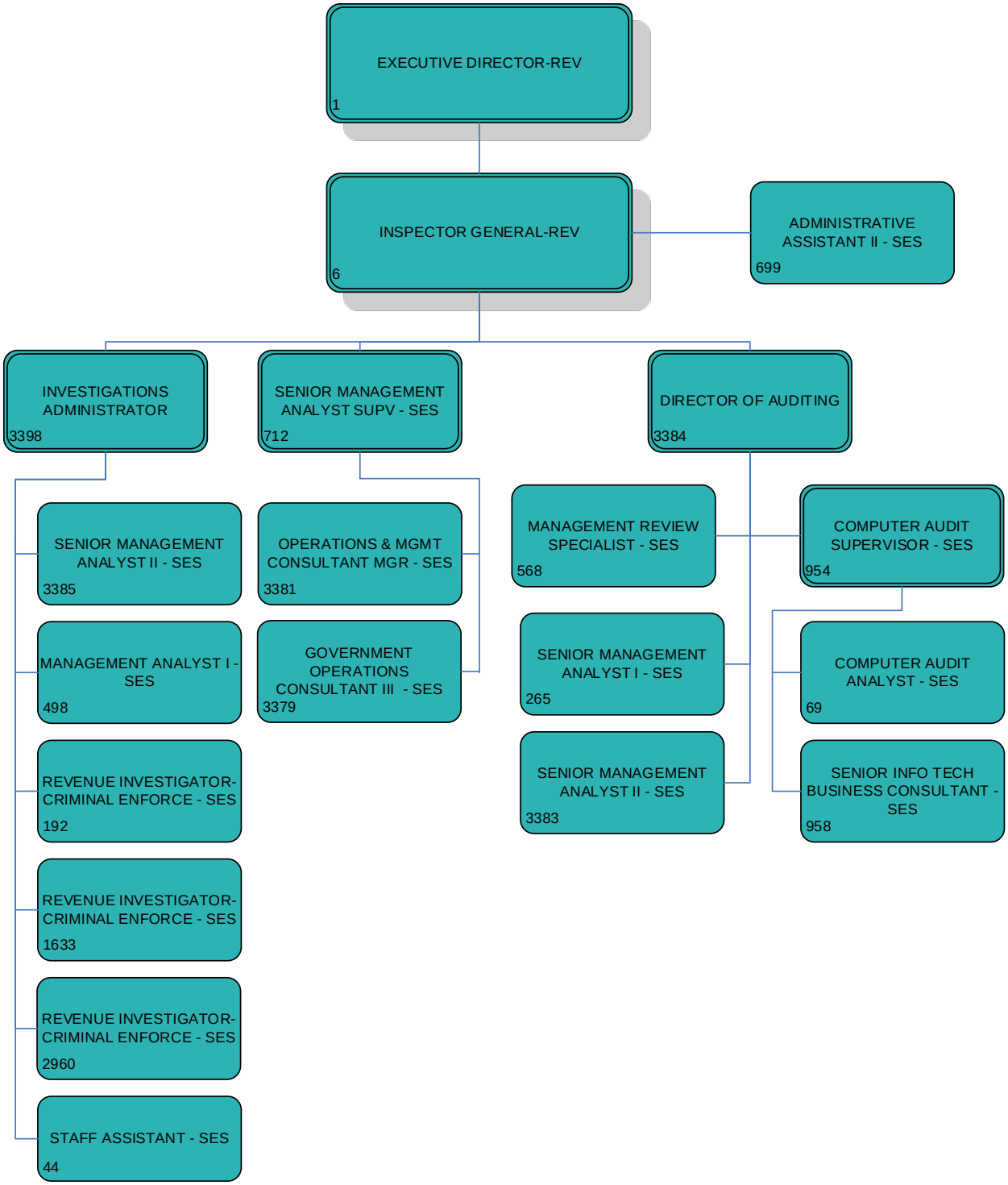
ANNUAL REPORT FY 2014-15

OFFICE OF INSPECTOR GENERAL

INTERNAL AUDITS · INTERNAL INVESTIGATIONS · SPECIAL PROJECTS

Table of Contents

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(8), 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, 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(6), F.S.

Additional laws relating to the OIG include:

- Sections 11.51(2) and (3), F.S. – Responses/follow-up for the OPPAGA (Office of Program Policy Analysis and Government Accountability) 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(7), 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.
- Coordinating Revenue's Fraud Prevention and Response Program.
- Carrying out other activities to promote economy and efficiency.

OIG Staff Certifications

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

Certifications	Number
Certified Florida Crime Prevention Practitioner – CFCPP	1
Florida Crime Prevention Through Environmental Design Practitioner	1
Certified Law Enforcement	1
Certified Fraud Examiner – CFE	5
Certified Information Systems Auditor – CISA	2
Certified Information Systems Security Professional – CISSP	1
Internal Auditor Certification in Information Technology Systems Management According to ISO/IEC 20000-1:2011	2
Certified Internal Auditor – CIA	3
Certified Inspector General – CIG	2
Certified Inspector General Auditor – CIGA	3
Certified Inspector General Investigator – CIGI	4
Six Sigma Yellow Belt Certified	4
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
- Florida Chapter of the Association 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
- ISACA (Formerly Known As Information Systems Audit and Control Association)
- FBI Law Enforcement Executive Development Association (LEEDA)
- InfraGard

Internal Audit Section

In accordance with section 20.055 (6), 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)[1] and consulting engagements in accordance with the *International Standards for the Professional Practice of Internal Auditing* (*Standards*), published by the Institute of Internal Auditors (IIA), and the *Principles and Standards for Offices of Inspector General*, published by the Association of Inspectors General.

Audit Services

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."

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:

- Reliability and integrity of information.
- Compliance with policies, procedures, laws, and regulations.
- Safeguarding assets.
- Economical 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. The OIG distributes audit reports internally to the Executive Director and affected Revenue managers and externally to the Office of the Auditor General (OAG).

[1] 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*.

Consulting Services

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. 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.

Other Services

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 about the progress of corrective action plans and verifies that corrective actions have resolved the issues on any findings management reported as completed. A report about 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(6)(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 about 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.

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.

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 if 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 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.

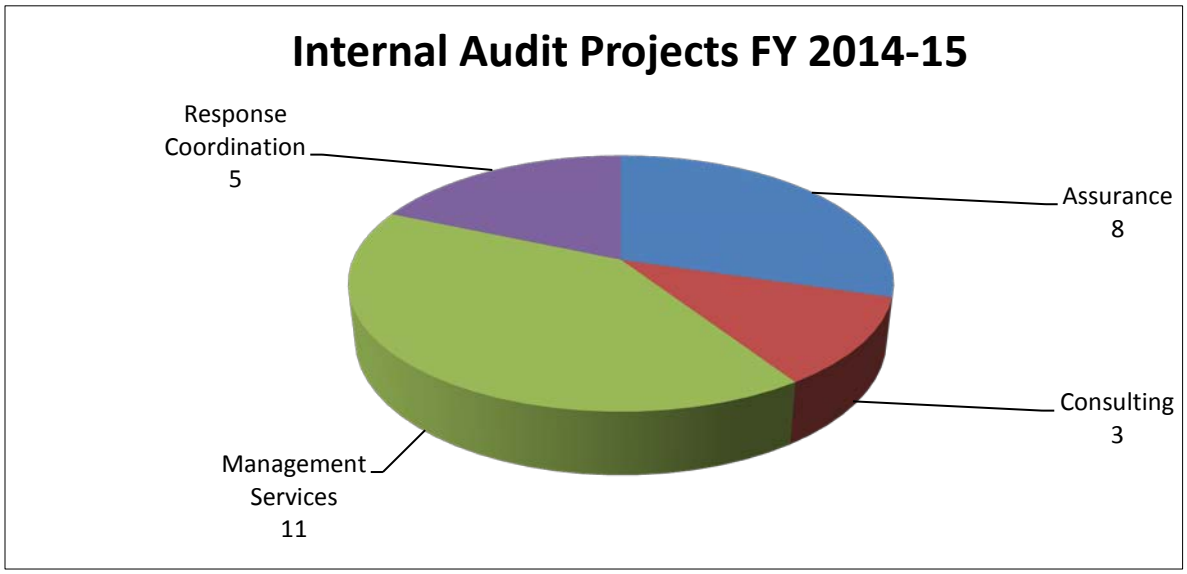
IAS Staff Certifications and Training

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 Computer Audit Supervisor, and the Director of Auditing. Professional designations held by staff within the IAS include Six Sigma-Yellow Belt, Certified Fraud Examiner, Certified Information Systems Auditor, Certified Inspector General Auditor, Certified Government Auditing Professional, ISO/IEC 20000 Associate Auditor, 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 an Association of Inspectors General training institute as well as local chapter meetings and training; Institute of Internal Auditors webinars as well as local chapter meetings and training sessions; ISACA (computer-related) training sessions; vendor-provided information technology, auditing, and management training; and department-provided employee training.

INTERNAL AUDIT PROJECTS

The following chart reflects the number of projects, by project type, completed during FY 2014/15. Detailed descriptions of the projects are included in the following section.



Assurance Engagements Conducted During FY 2014/15

During FY 2014/15, the IAS completed 8 assurance engagements. Below is a summary of activity for the year.

Child Support Program (CSP) Establishment – Support Order Establishment and Modification

The objectives of this audit were to determine whether:

- Private Legal Service Providers (LSP) are in compliance with selected contract requirements.
- LSPs are being monitored effectively.

The audit concluded that:

- LSP contract compliance could be improved.
- Monitoring activities conducted by CSP Contract Management should be improved to ensure LSPs perform according to contract terms.

CSP Establishment – Paternity Establishment

The objective of the audit was to determine if controls related to collecting samples for genetic testing in Revenue's service centers is adequate.

The audit concluded that physical control over testing supplies and DNA collection samples is not adequate.

CSP Payment Data Processing – Trust Fund Distribution
The objective of this audit was to determine whether the internal controls in place for managing the CSP Payment Data Processing Trust Fund Distribution sub-process are adequate.

The audit concluded:

- In four of the five control areas reviewed, internal controls are generally functioning properly to provide reasonable assurance that management's goals and objectives are met for the trust fund distribution process.
- Written policies and procedures for the Trust Fund Distribution sub-process are not adequate.

General Tax Administration Program (GTA) – Taxpayer Services
The objective of the audit was to determine whether internal controls over compromises and corrections of tax, penalty, and interest are sufficient and effective.

The audit concluded, while the information processing application control appeared adequate and functioning as designed, other controls related to compromises and corrections could be improved:

- While compromise information is being provided to the Governor and Cabinet as required by Florida Administrative Code, the information is incomplete.
- While the quality review program is working as detailed in GTA Collections Process Procedure Section 1.18, the high error rates suggest that follow-up training is not sufficient.

GTA Return Processing and Fund Distribution – Refund Determination
The objective of this audit was to evaluate the refund approval process to determine whether internal controls are adequate and provide reasonable assurance the correct refund amount is paid to the appropriate taxpayer.

The audit concluded:

- In general, internal controls are functioning properly to provide reasonable assurance that management's goals and objectives are met for the refund determination process.
- The SUNTAX system change process in GTA is functioning properly and coordinated with the Information Services Program (ISP) Change Control process.
- The special mailing request process implemented between refund determination and the vouching process is working as intended.

- A second review of all refund determinations that meet the quality assurance review process thresholds, approved or denied, should be conducted for newly hired or promoted employees to verify training received is effective.
- The process owners of the Refund Determination Unit should conduct periodic reviews of the SUNTAX user access permissions for all employees in the workgroup and remove unnecessary system access to minimize the security risk to the SUNTAX system.

GTA Receivables Management - Enforcement
The objectives of this audit were to:

- Determine whether selected performance measures being reported are valid and reliable.
- Determine whether liens, bank freezes, garnishments, levies, and warrants are completed consistently.
- Determine whether write-off methodologies are consistently applied from case to case.

The audit concluded:

- While performance measures appear to be valid, performance goals and data reliability could be improved.
- While GTA completed enforcement actions consistently, not all enforcement-related procedures are consistent with current business processes.
- Write-off methodologies were generally applied consistently.

GTA Compliance Determination
The objectives of this audit were to:

- Determine if selected Long Range Program Plan performance measures related to Compliance Determination are valid and reliable.
- Determine whether sales and use tax audits are completed within statutory time requirements.

The audit concluded:

- Performance measures appear to be valid and reliable.
- The “Notice of Proposed Assessment” was not always issued within one year from the issue date of the “Notification of Intent to Audit Books and Records” (DR-840).

Technical Assistance and Dispute Resolution (TADR)
The objective of the audit was to follow up on two findings from Report No. 2008-0113-A to determine if corrections were made:

- Approval authority for compromises made by TADR was not always authorized and adequately documented.
- Checks were not immediately logged into the check log upon receipt in TADR.

The audit concluded that:

- Approval authority for compromises made by TADR was properly authorized and adequately documented with two exceptions. Additionally, subsequent closing agreements were not always properly prepared by TADR or completed by the taxpayer.
- Payments received by TADR were logged into the check log, deposited timely, and logged into SUNTAX; however, detailed written procedures should be established to ensure consistent check handling.

Consulting Engagements Conducted During FY 2014/15
During FY 2014/15, the IAS completed three consulting engagements. Below is a summary of consulting engagements conducted.

CSP Payment Processing Analysis
The purpose of this engagement was to review the CSP payment processing flow from receipt at the State Disbursement Unit through payment disbursement for:

- Internal control weaknesses.
- Risk levels and a priority for corrective actions.
- Possible risk reduction strategies and activities.

GTA Account Management File Review
The purpose of this engagement was to review the files and processes related to Account Management's criminal history record check process for compliance with Florida Department of Law Enforcement contract requirements.

Enterprise Team - Hiring and Developing Auditors
The Director of Auditing served on a team composed of audit directors from state and local government agencies. The purpose of the team was to develop materials related to hiring and developing internal auditors. Topics addressed by the team were best practices for recruiting, interviewing, and training auditors.

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 one forensic review of computers, by pulling information from Revenue's information systems and providing analysis of data.

IAS staff acted as agency coordinator for the Florida Single Audit Act (FSAA). This function included acting as liaison with program FSAA leads, helping identify legislative effects on Revenue related to the FSAA, and handling inquiries from the public or other state agencies. IAS was also 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 seven external audits conducted by other entities, and coordinated Revenue's responses to those audits when necessary.

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

Follow-Up on Corrective Action Plans as of 6/30/2014
The purpose of this review was to follow up on the programs' assertions for the corrective action plans as of June 30, 2014. A summary report was provided to the Executive Director indicating there were 51 open findings, 17 findings verified by OIG staff as closed during the period, and 36 corrective actions overdue.

Follow-Up on Corrective Action Plans as of 12/31/14
The purpose of this engagement was to follow up on the program assertions for the corrective action plans as of December 31, 2014. A summary report was provided to the Executive Director indicating there were 43 open findings, 19 findings verified by OIG staff as closed during the period, and 35 corrective actions overdue.

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

LBR/LRPP Performance Measures Review FY 2014/15
The purpose of this review was to assess the reliability and validity of new performance measures requested in the Long Range Program Plan (LRPP) submitted in conjunction with the Legislative Budget Request (LBR).

<u>Other IAS Accomplishments During FY 2014/15</u>
In addition to the reports and activities listed above, the IAS accomplished the following during FY 2014/15:

- Received a quality assurance review from the Auditor General that resulted in no findings.
- Staff completed training that will enhance the efficiency and effectiveness of the internal audit function, including the following:
    - Two staff members received the ISO/IEC 20000 Associate Auditor designation.
    - One staff member received the Certified Inspector General Auditor designation.

    - One staff member received the Certified Information Systems Auditor designation.
    - One staff member completed four parts of the Certified Public Manager course, and is eligible for the Certified Supervisory Manager designation.
- Assisted the Inspector General community by serving on a committee to produce the Tallahassee Chapter of the Institute of Internal Auditors' quarterly newsletter.
- 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. The IIS is also responsible for investigating waste and abuse involving Revenue employees, vendors, contractors, or consultants. 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 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.

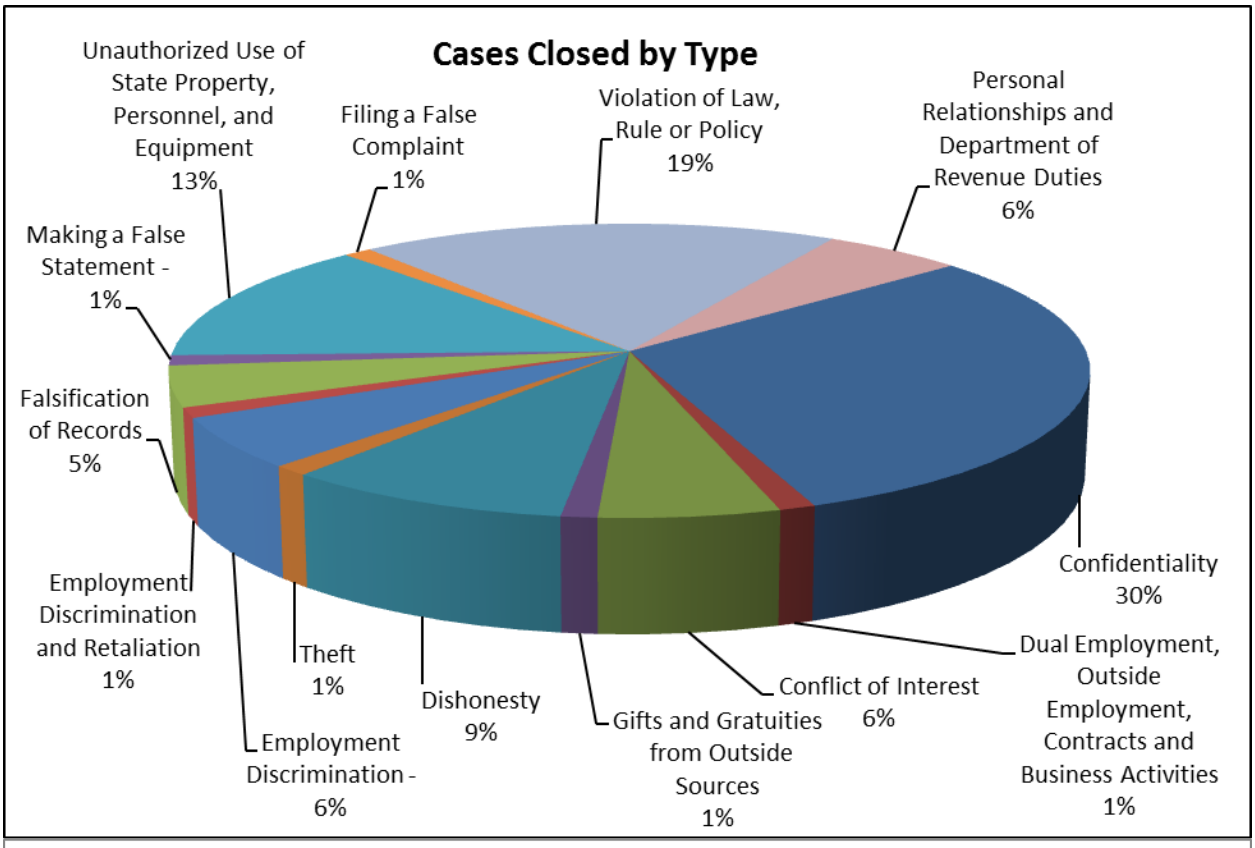
IIS staff conducts a preliminary review of each complaint received by the OIG. The preliminary review process serves to filter complaints to ensure that investigative resources are used effectively and efficiently. Established criteria are used to initially evaluate each complaint to determine the appropriate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

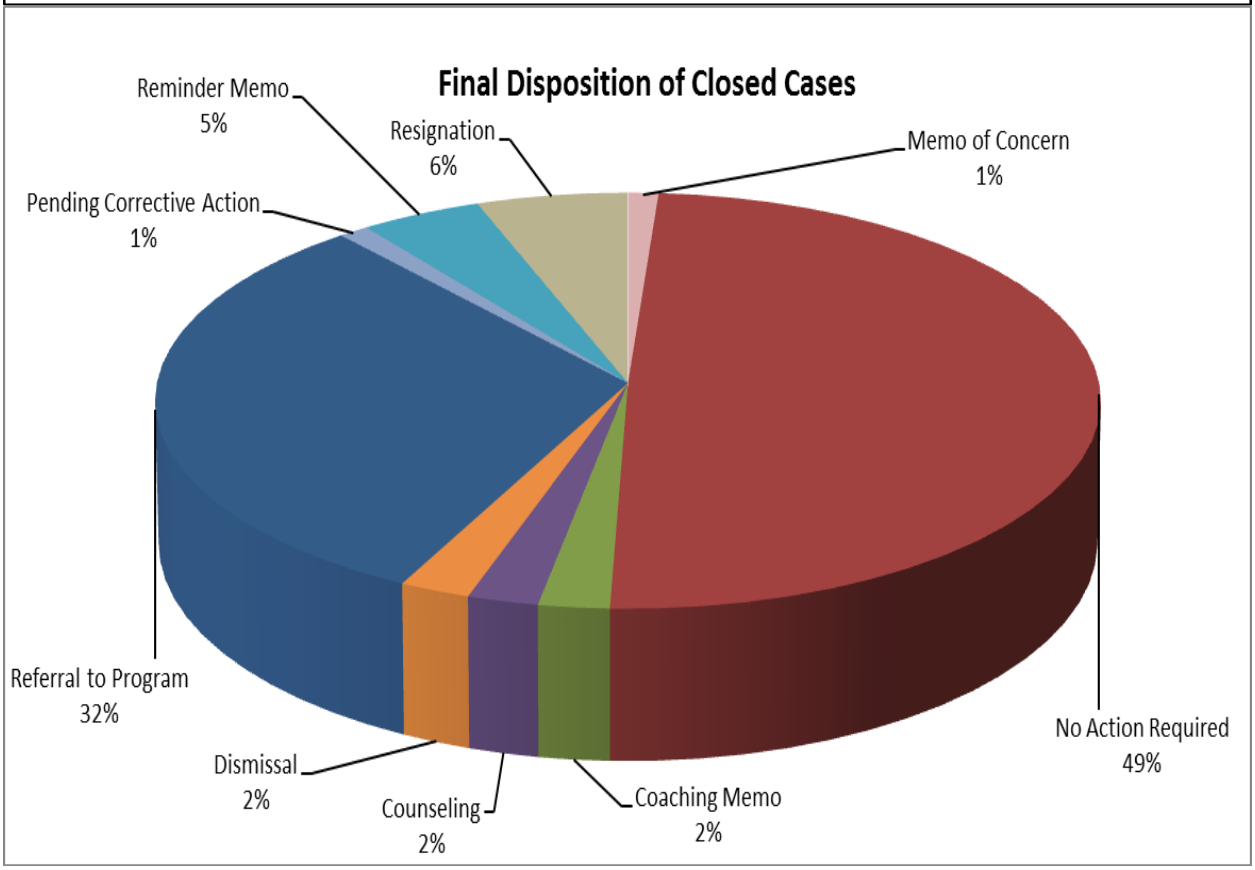
IIS Accomplishments During FY 2014/15

- Several staff members completed 21 hours of Equal Employment Opportunity (EEO) Investigator training sponsored by the Tallahassee Chapter of Internal Auditors.
- Several staff members attended an eight-hour "Writing and Editing Workshop for Inspector General Offices" sponsored by the Florida Chapter of the Association of Inspectors General.
- One staff member completed the Reid Technique Interviewing and Interrogation course.
- One staff member completed four parts of the Certified Public Manager course, and is eligible for the Certified Supervisory Manager designation.
- Held periodic meetings with the accreditation manager to ensure the *IIS Policies and Procedures Manual* is current and in compliance with the Commission for Florida Law Enforcement Accreditation (CFA) standards.

IIS completed 29 investigations and 60 preliminary reviews during FY 2014/15.

The following charts reflect the types and outcomes of cases closed, including both preliminary reviews and investigations, during FY 2014/15.


Cases Closed by Type
Unauthorized Use of State Property, Personnel, and Equipment 13%
Filing a False Complaint 1%
Violation of Law, Rule or Policy 19%
Personal Relationships and Department of Revenue Duties 6%
Making a False Statement - 1%
Falsification of Records 5%
Confidentiality 30%
Employment Discrimination and Retaliation 1%
Theft 1%
Dishonesty 9%
Conflict of Interest 6%
Dual Employment, Outside Employment, Contracts and Business Activities 1%
Employment Discrimination - 6%
Gifts and Gratuities from Outside Sources 1%


Final Disposition of Closed Cases
Reminder Memo 5%
Resignation 6%
Memo of Concern 1%
Pending Corrective Action 1%
Referral to Program 32%
No Action Required 49%
Dismissal 2%
Counseling 2%
Coaching Memo 2%

Investigation Summaries for FY 2014/15

A number of significant investigations were conducted during FY 2014/15. The following are highlights of some of these cases:

Confidentiality

The OIG received allegations from a person owed child support that a Revenue employee may have viewed her case in the child support computer system to obtain confidential information for purposes not related to her job. During the OIG investigation, the employee admitted to accessing and viewing the case information for unauthorized purposes, photographing the information that appeared on the computer screen, and then texting the picture to the person owing child support on the case using her personal cell phone. The employee disclosed that she had a long term dating relationship with the person owing support and texted the information to him to prove he had lied to her about a personal matter. In addition, the employee admitted she used another agency's computer system she had authorized access to for purposes not related to her job. The employee was dismissed.

Unauthorized Use of State Property, Personnel, and Equipment

The OIG received information from Revenue's Confidential Incident Response and Disclosure Officer, that management reported finding confidential information on a Post-it note on the ground in the office parking lot and identified the handwriting as that belonging to a Revenue employee assigned to that office. The OIG was also notified by management that the employee maintained an unsecured folder containing personal information as well as confidential work-related documents. In addition management informed the OIG that the employee made statements to other employees in the office, and that a Twitter account was established using Revenue e-mail. The investigation could not determine how the Post-it note containing confidential information ended up on the ground in the parking lot. The investigation also did not find that the employee established a Twitter account using Revenue e-mail, or recorded or copied confidential information for unauthorized or illicit purposes. Based on the findings in the investigation, no disciplinary action was warranted.

Violation of Law Rule or Policy

The OIG received an anonymous letter that a Revenue manager shared inappropriate photos she had on her personal cell phone with several of the individuals she supervised in the workplace. The investigation substantiated the allegation and found the manager violated Revenue's Non-Discrimination Policy and Complaint Procedure. The manager resigned from her position.

Falsification of Records

The OIG received a complaint from management that a Revenue employee allegedly used a supervisor's signature without authorization by cutting and pasting the supervisor's signature to official documents. The official documents were used to either clear or place holds on customers' bank accounts for delinquent taxes. The investigation determined the employee did falsify the supervisor's signature and also, without authorization, signed another supervisor's signature to an official document. The investigation also determined the employee was

untruthful during her OIG interview. Her unauthorized use of her supervisors' signatures was done to reverse holds that were placed on customers' accounts in error or holds that were duplicative. Corrective action is pending.

Confidentiality

The OIG received information from management that an employee may have interfered with the processing of a child support case and the reinstatement of the driver's license of a person owing child support. The person owing child support alleged a family relationship between the employee and the person owed child support and that the employee may have accessed their child support case. The investigation determined the employee did not interfere with the processing of the case but did access the case on several different occasions without authorization from his supervisor. Additionally, the investigation found that the employee did not disclose to management that he had a family relationship with one of the parties listed on the case. The employee received corrective action.

Personal Relationships

The OIG received a complaint from a person owed child support alleging that an employee was a relative of the person owing support on the case. The person owed support also alleged the employee viewed the case in the child support computer system without supervisor authorization and changed a mailing address. The investigation revealed that the employee, as part of her work responsibilities, accessed the child support case in the system, however, once the employee discovered that she was related to one of parties named in the case, she immediately reported her actions to management and the case was reassigned. The investigation also determined the employee did not change the address, but rather the address change was initiated by a computer system in another agency that interfaced with the child support system. Unrelated to the initial allegation, the investigation found that the employee, while training another employee, allowed the employee to train using her computer log on credentials. This information was referred to management to address.

See Appendix B for a summary of closed cases for FY 2014/15, 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 proposed 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.

SPS Accomplishments During FY 2014/15

- Finalized and implemented an agency-wide *Fraud Prevention and Response Policy*.
- Conducted fraud awareness presentations for 64% of managers within the agency.
- Incorporated a fraud awareness training component into the agency's new supervisor orientation process.
- One staff member attained the Certified Fraud Examiner delegation through the Association of Certified Fraud Examiners.
- Developed and implemented a fraud awareness campaign to coincide with International Fraud Awareness Week.
- Coordinated development and deployment of *Identifying and Responding to Violence in the Workplace* training for all agency employees and on-site contractors' staff.

Workplace Violence

Revenue'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. 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 parent owing support in a child support case threatening to harm the parent owed support 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.

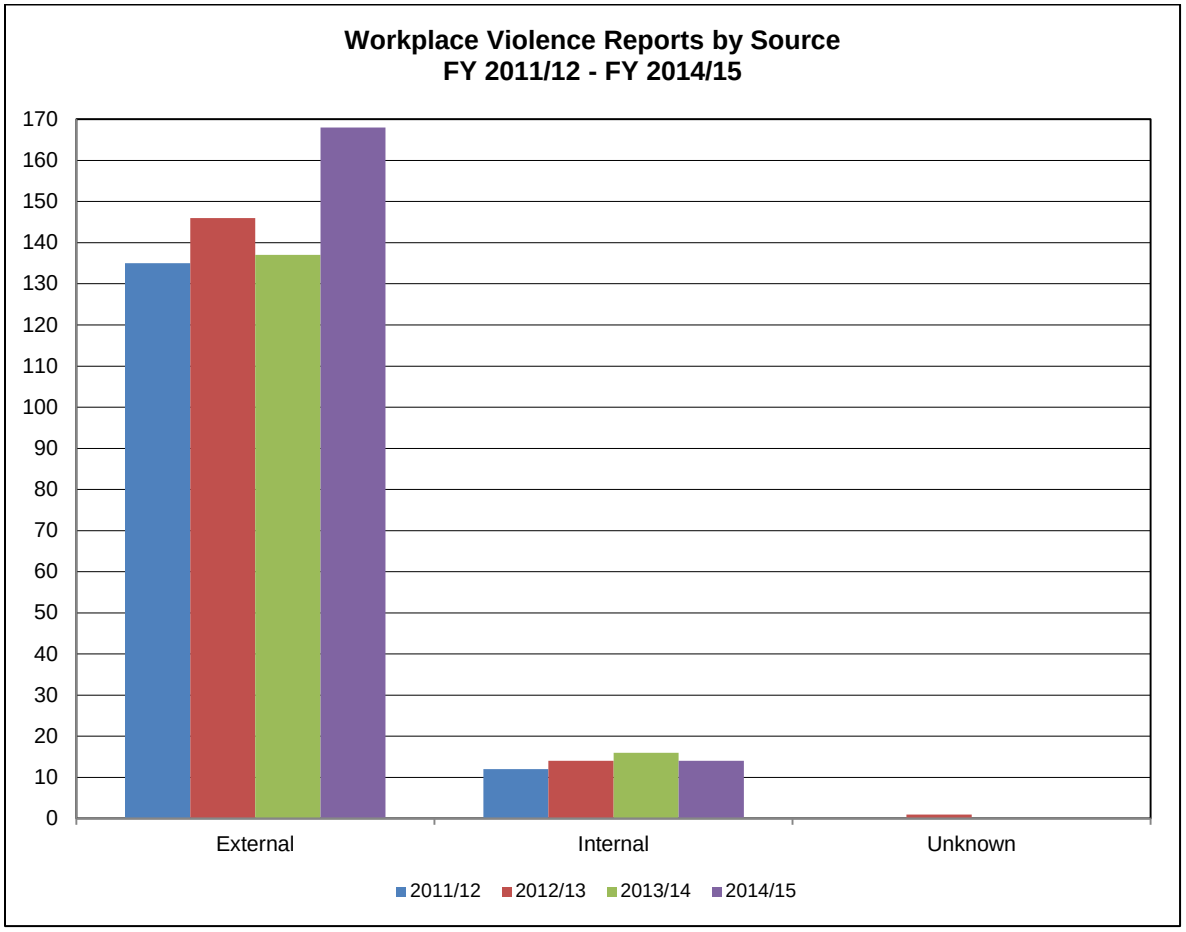
When it is determined that a potentially violent person may be associated with a tax account or child support case, a Potentially Dangerous Contact (PDC) indicator is placed on applicable primary databases used within the operating programs of Revenue. This indicator flag serves as notice to an employee 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 and child support administration responsibilities are carried out in relation to a PDC account.

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. A domestic violence concern 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

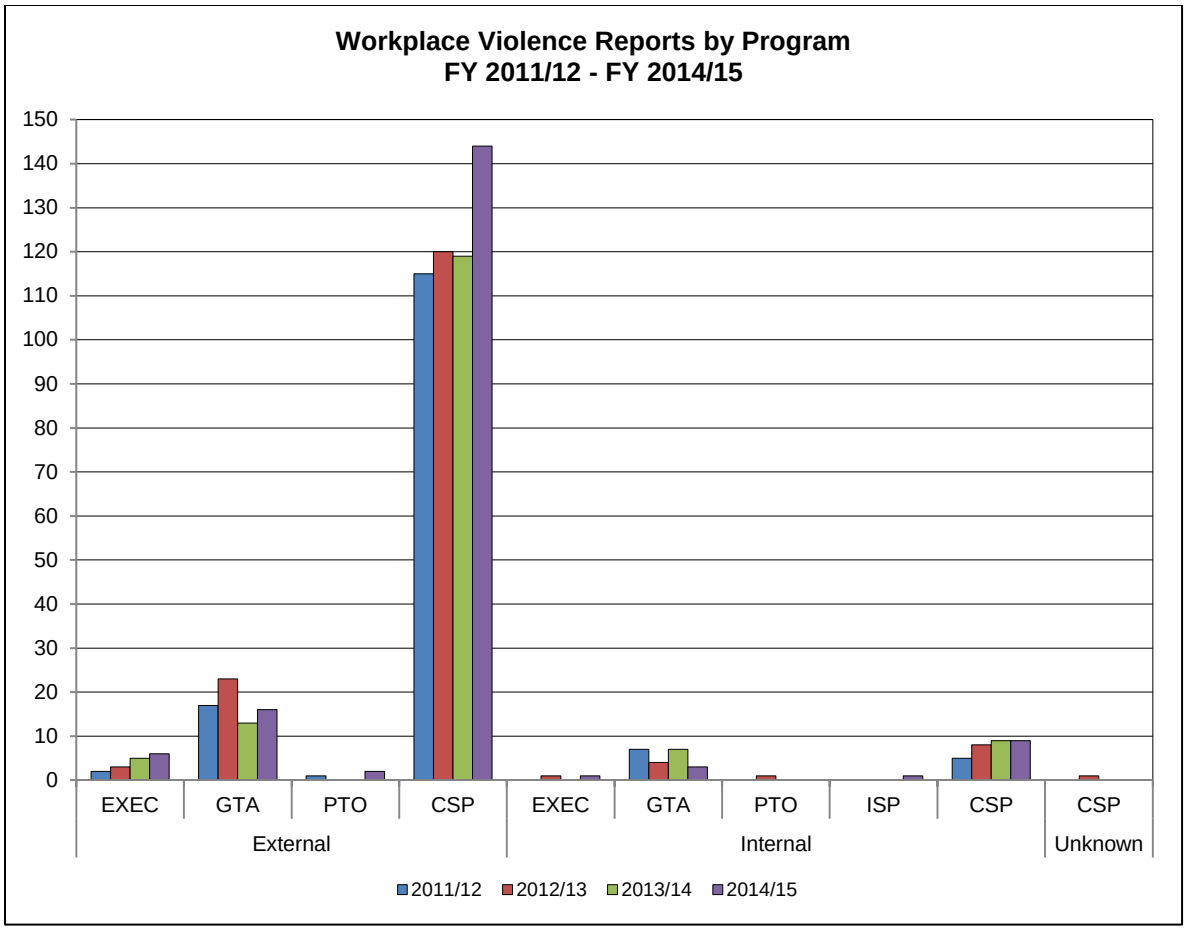
any concern that the respondent may come to the workplace. The SPS works with appropriate management to take necessary actions to protect victims of domestic violence in the workplace, as well as to help ensure the safety of the victim's co-workers. The WPV Team may be convened if needed to address more 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 182 reports of workplace violence were received during FY 2014/15, an increase from the 153 incidents reported during the previous fiscal year. Fourteen of these incidents involved a Revenue employee as the perpetrator, compared to 16 in the previous fiscal year.

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



During FY 2014/15, CSP reported 144 incidents from external sources and 9 incidents from internal sources, GTA reported 16 incidents from external sources and 3 incidents from internal sources, EXE reported 6 incidents from external sources and 1 incident from an internal source, the Property Tax Oversight Program (PTO) reported 2 incidents from external sources and no incidents from an external source, and ISP reported 1 incident from an internal source and no incidents from an external source.

The SPS continually seeks methods and strategies to combat workplace violence and apply them in our day-to-day activities. During this fiscal year, SPS staff coordinated the development and deployment of training to provide staff and management guidance on how to react to an irate customer exhibiting a variety of specific behaviors to defuse the situation before it becomes violent. The training also provides options for an employee to consider if confronted with an active shooter situation.

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.

Thirty current arrest reports were received and 39 current arrest follow-up review cases were closed during the fiscal year.

Ten 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 champion an agency-wide fraud prevention and response program for Revenue. The first step was to draft a 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 actions to take if they suspect fraudulent activity within or affecting Revenue services.

Revenue's Strategic Leadership Board (SLB) approved the *Fraud Prevention and Response Policy* during their July 17, 2014, meeting and established a September 1, 2014, effective date. To accompany the policy, four internal web-based reporting forms were developed to provide an avenue for reporting allegations of suspected fraud involving child support, tax administration, property tax oversight, and occupational fraud committed by Revenue employees, contractors, or vendors. These reporting forms allow employees or contractors' employees to report concerns anonymously or by providing their names.

During FY 2014/15, SPS staff:

- Delivered 23 fraud awareness presentations to Revenue managers.
- Participated in the Internal Audit Section's annual risk assessment. A fraud risk category is included in 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.
- Provided data analysis assistance to FDLE and the Internal Investigations Section in their investigation of an alleged check fraud scheme related to child support payments. The project included various phases of analyses and research including names and addresses of customers owing and customers owed support, financial information, geographical mapping, and payment and disbursement analyses. Staff provided recommendations to program management to enhance payment processing internal controls.
- Researched and developed various periodic tests using data analytics to detect purchasing card fraud. The periodic tests are designed to support controls to detect and promptly pinpoint potential fraud. This project is still in progress.

Appendix A

Outstanding Corrective Actions for Prior Audit Reports

IAS Engagements Outstanding Corrective Actions as of 6/30/2015		
Report Number	**Project Name**	**Recommendation**
2007-0067	Internet Tax Applications	Confidential 2-2
2007-0067	Internet Tax Applications	Confidential 2-3
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, Florida Administrative Code, 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.
2009-0107 A	Contract Management Process	1.2 We recommend the Purchasing and Contract Management Manual include specific procedures and requirements 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.
2009-0107 A	Contract Management Process	3. We recommend Purchasing Process management require contract managers to enter the necessary information in CATS 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.

IAS Engagements Outstanding Corrective Actions as of 6/30/2015		
2009-0113-A	ISP/Agency Application Management-Requirements	1. We recommend ISP request assistance through the Strategic Leadership Board 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 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.
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
2010-0120-A2	GTA Pittsburgh Out-of-State Service Center-Confidential	1.2 Confidential
2010-0121-A2	GTA In-State Service	1.2 Confidential

IAS Engagements Outstanding Corrective Actions as of 6/30/2015		
	Centers - Miami, Coral Springs, West Palm Beach-Confidential	
2010-0121-A2	GTA In-State Service Centers - Miami, Coral Springs, West Palm Beach-Confidential	1.2 Confidential
2010-0121-A2	GTA In-State Service Centers - Miami, Coral Springs, West Palm Beach-Confidential	1.4 Confidential
2010-0121-A2	GTA In-State Service Centers - Miami, Coral Springs, West Palm Beach-Confidential	1.4 Confidential
2010-0121-A2	GTA In-State Service Centers - Miami, Coral Springs, West Palm Beach-Confidential	1.4 Confidential
2011-0106-A1	CSP Payment Processing - Fund Distribution	1. The Department should consider reconciling the daily disbursement instruction file sent to the State Disbursement Unit 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
2011-0134-A2	CSP, GTA, PTO Tampa Service Centers - Confidential	1.1 Confidential
2011-0135-A2	CSP and GTA Port Richey	1.1 Confidential

IAS Engagements Outstanding Corrective Actions as of 6/30/2015		
	Service Centers - 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
2012-0115	Department-Wide Data Security	2(a) Confidential
2012-0115	Department-Wide Data Security	2(b) Confidential
2012-0108	GTA Compliance Determination	GTA should review the best practices being utilized in Regions III and V, which have resulted in a higher level of compliance, and apply those practices to other regions.
2013-0117	GTA Return Processing and Fund Distribution	We recommend that the second review of all refund determinations, approved or denied, be conducted for newly hired or promoted employees, to verify training received is followed.
2013-0117	GTA Return Processing and Fund Distribution	We recommend GTA expand the Quality Assurance Review selection process to include denied refund cases for completeness.
2013-0117	GTA Return Processing and Fund Distribution	The process owners of the Refund Determination unit should conduct periodic reviews of the SUNTAX user access permissions for all employees in the workgroup and remove unnecessary system access to minimize the security risk to the SUNTAX system.
2013-0138	CSP Payment Data Processing - Trust Fund Distribution	The process owner and manager of the CSP Trust Fund Distribution Unit should continue their efforts to enhance the current job aids by creating and publishing written policies and procedures.
2013-0135	GTA Receivables Management - Enforcement	1. Percent of Delinquent Accounts Reaching Uncollectible Status: GTA has improved the procedure for measurement of “percent of delinquent accounts

IAS Engagements Outstanding Corrective Actions as of 6/30/2015		
		reaching uncollectible status," by writing a query to extract the numerator used in calculating the ratio, rather than doing it manually. GTA should test this new query process to ensure the new methodology provides reliable results.
2013-0135	GTA Receivables Management - Enforcement	2. Number of Billings Resolved: GTA has automated the queries to minimize possible human error related to the reporting process. To further ensure that the data is reliable and auditable, we recommend that GTA consult with ISP to explore cost-effective options for storing data used to calculate this measure.
2013-0135	GTA Receivables Management - Enforcement	GTA currently has a repair order to correct the system functionality problem wherein auto warrants for Corporate Income Tax (CIT) sometimes do not hit the Comment History Screen. GTA should ensure that this repair order is completed on a timely basis.
2013-0136	CSP Establishment - Support Order Establishment & Modification	Legal Service Providers (LSPs) should ensure complete and accurate information is entered into CAMS and supporting documentation is retained.
2013-0136	CSP Establishment - Support Order Establishment & Modification	CSP should enforce the provision to use CAMS-generated forms, or the provision should be deleted from the contract.

IAS Engagements Outstanding Corrective Actions as of 6/30/2015		
2013-0136	CSP Establishment - Support Order Establishment & Modification	LSPs should work with Contract Management to ensure all required classes are completed by their staff members prior to accessing Department information resources. CSP Contract Management should continue to work with the vendor, Office of Workforce Management, and ISP to resolve connectivity issues for LSP external users of the Learning Management System (LMS). A workaround for the LMS connectivity problem is in place, and CSP Contract Management, LMS staff, and ISP are seeking a permanent solution. CSP Contract Management should ensure all provisions of the contract are enforced.
2013-0136	CSP Establishment - Support Order Establishment & Modification	LSPs should comply with CSP contract requirements to provide monthly lists of employees with access to DOR information resources. Contract Management should ensure all provisions of the contract are enforced.
2013-0136	CSP Establishment - Support Order Establishment & Modification	LSPs should ensure CSP Contract Management is notified within three business days, as noted in the contract, when an employee with CAMS access terminates employment.
2013-0136	CSP Establishment - Support Order Establishment & Modification	The LSPs should work with CSP Contract Management to ensure criminal background checks are completed for all staff, employees, and subcontractor staff that have contact with Department information resources unless the Department has formally waived this requirement in writing. Future LSP contracts should clarify criminal background check requirements for LSP staff, employees, and subcontractor staff that have access to Department information resources.

IAS Engagements Outstanding Corrective Actions as of 6/30/2015		
2013-0136	CSP Establishment - Support Order Establishment & Modification	LSPs should ensure that all laptops and mobile devices used to access or store Department information resources are properly encrypted. CSP should ensure the Department's specific encryption standard for laptops and mobile devices is implemented on LSP laptops and devices storing confidential information.
2013-0136	CSP Establishment - Support Order Establishment & Modification	CSP Contract Management should implement procedures to improve monitoring of LSP compliance with contract requirements. CSP Contract Management should continue to work with Enterprise System Support Process (ESSP) personnel to ensure the usability of PAMs reports for performance monitoring or develop alternative methods to measure performance.
2014-0100	General Tax Administration Program - Taxpayer Services	GTA should run a centralized business intelligence report to capture all compromises over $50,000.
2014-0100	General Tax Administration Program - Taxpayer Services	GTA should study the feasibility of integrating compromises performed by Technical Assistance & Dispute Resolution (TADR) and Office of the General Counsel in SUNTAX/SAP in a format that can be reported in business intelligence reports.
2014-0100	General Tax Administration Program - Taxpayer Services	Management should establish methodology to educate all agents in a timely fashion concerning trends of errors gleaned from the quality review program.
2014-0100	General Tax Administration Program - Taxpayer Services	Management should strengthen training related to reason codes for collectors and managers.
2014-0118	Technical Assistance and Dispute Resolution (TADR)	TADR should establish written procedures to ensure all compromises are properly authorized and adequately documented and all closing agreements are properly prepared and completed.
2014-0118	Technical Assistance and Dispute Resolution	TADR should establish a written check handling procedure that includes all steps and responsibilities in the check handling process.

IAS Engagements Outstanding Corrective Actions as of 6/30/2015		
2014-0114	CSP Establishment - Paternity Establishment	Management should update job aids to mirror procedures that require collection samples be kept in a locked environment when not in the possession of the collector.

Appendix B

Summary of Closed Internal Investigations for FY 2014/15

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

Project Number	Disposition	Type
13012	Unsubstantiated	Conflict of Interest
13125	Referral	Dishonesty
13148	Substantiated	Unauthorized Use of State Property, Personnel, and Equipment
13166	Substantiated	Confidentiality
13179	Unsubstantiated	Falsification of Records
13193	Substantiated	Confidentiality
13197	Referral	Violation of Law, Rule, or Policy
13205	Referral	Violation of Law, Rule, or Policy
13218	Substantiated	Confidentiality
13239	Referral	Personal Relationships and Department of Revenue Duties
13240	Unsubstantiated	Conflict of Interest
13241	Referral	Conflict of Interest
13245	Unsubstantiated	Dishonesty
13247	Referral	Personal Relationships and Department of Revenue Duties
13251	Referral	Personal Relationships and Department of Revenue Duties
13256	Referral	Violation of Law, Rule, or Policy
13264	Substantiated	Confidentiality
13267	Referral	Dishonesty
13276	Substantiated	Violation of Law, Rule, or Policy
13277	Unsubstantiated	Unauthorized Use of State Property, Personnel, and Equipment
13278	Unsubstantiated	Unauthorized Use of State Property, Personnel, and Equipment
13279	Unsubstantiated	Violation of Law, Rule, or Policy
13281	Substantiated	Confidentiality
13290	Unsubstantiated	Confidentiality
13293	Unsubstantiated	Confidentiality
13298	Substantiated	Violation of Law, Rule or Policy
14001	Unsubstantiated	Confidentiality
14002	Unsubstantiated	Confidentiality
14007	Unsubstantiated	Filing a False Complaint
14010	Unsubstantiated	Violation of Law, Rule, or Policy
14013	Substantiated	Confidentiality
14016	Unsubstantiated	Confidentiality
14020	Unsubstantiated	Personal Relationships and Department of Revenue Duties

Project Number	Disposition	Type
14021	Substantiated	Employment Discrimination
14022	Unsubstantiated	Dishonesty
14034	Unsubstantiated	Violation of Law, Rule, or Policy
14036	Unsubstantiated	Dishonesty
14037	Unsubstantiated	Confidentiality
14040	Substantiated	Conflict of Interest
14042	Substantiated	Confidentiality
14047	Referral	Unauthorized Use of State Property, Personnel, and Equipment
14049	Referral	Confidentiality
14057	Referral	Dishonesty
14058	Substantiated	Falsification of Records
14060	Unsubstantiated	Violation of Law, Rule, or Policy
14063	Referral	Violation of Law, Rule, or Policy
14071	Unsubstantiated	Unauthorized Use of State Property, Personnel, and Equipment
14073	Unsubstantiated	Confidentiality
14074	Referral	Falsification of Records
14075	Unsubstantiated	Violation of Law, Rule, or Policy
14077	Unsubstantiated	Confidentiality
14079	Unsubstantiated	Confidentiality
14086	Referral	Confidentiality
14087	Referral	Confidentiality
14092	Referral	Falsification of Records
14094	Unsubstantiated	Gifts and Gratuities from Outside Sources
14095	Unsubstantiated	Violation of Law, Rule or Policy
14106	Substantiated	Confidentiality
14108	Unsubstantiated	Confidentiality
14112	Unsubstantiated	Violation of Law, Rule, or Policy
14115	Referral	Violation of Law, Rule, or Policy
14118	Unsubstantiated	Confidentiality
14125	Substantiated	Unauthorized Use of State Property, Personnel, and Equipment
14128	Unsubstantiated	Dishonesty
14133	Substantiated	Confidentiality
14134	Substantiated	Employment Discrimination
14135	Referral	Violation of Law, Rule, or Policy
14143	Unsubstantiated	Unauthorized Use of State Property, Personnel, and Equipment
14145	Unsubstantiated	Violation of Law, Rule, or Policy
14148	Unsubstantiated	Confidentiality
14149	Unsubstantiated	Confidentiality

Project Number	Disposition	Type
14150	Referral	Unauthorized Use of State Property, Personnel, and Equipment
14155	Unsubstantiated	Personal Relationships and Department of Revenue Duties
14160	Referral	Conflict of Interest
14171	Unsubstantiated	Employment Discrimination
14172	Referral	Confidentiality
14182	Referral	Dishonesty
14198	Substantiated	Employment Discrimination
14199	Unsubstantiated	Unauthorized Use of State Property, Personnel, and Equipment
14210	Referral	Violation of Law, Rule, or Policy
14211	Unsubstantiated	Employment Discrimination
14225	Unsubstantiated	Unauthorized Use of State Property, Personnel, and Equipment
14230	Unsubstantiated	Confidentiality
14233	Substantiated	Dual Employment, Outside Employment, Contracts, and Business Activities
14237	Unsubstantiated	Theft
14257	Substantiated	Unauthorized Use of State Property, Personnel, and Equipment
14258	Unsubstantiated	Employment Discrimination and Retaliation
14300	Referral	Making a False Statement
14322	Referral	Unauthorized Use of State Property, Personnel, and Equipment

FLORIDA DEPARTMENT OF REVENUE

WWW.MYFLORIDA.COM/DOR