




Executive
Director
Marshall Stranburg

September 24, 2013

MEMORANDUM

TO: Marshall Stranburg, Executive Director

FROM: Sharon Doredant, Inspector General 

SUBJECT: Annual Report for Fiscal Year 2012/13

We are pleased to submit the Office of Inspector General's (OIG) Annual Report for the fiscal year ending June 30, 2013. 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/bh

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

Annual Report

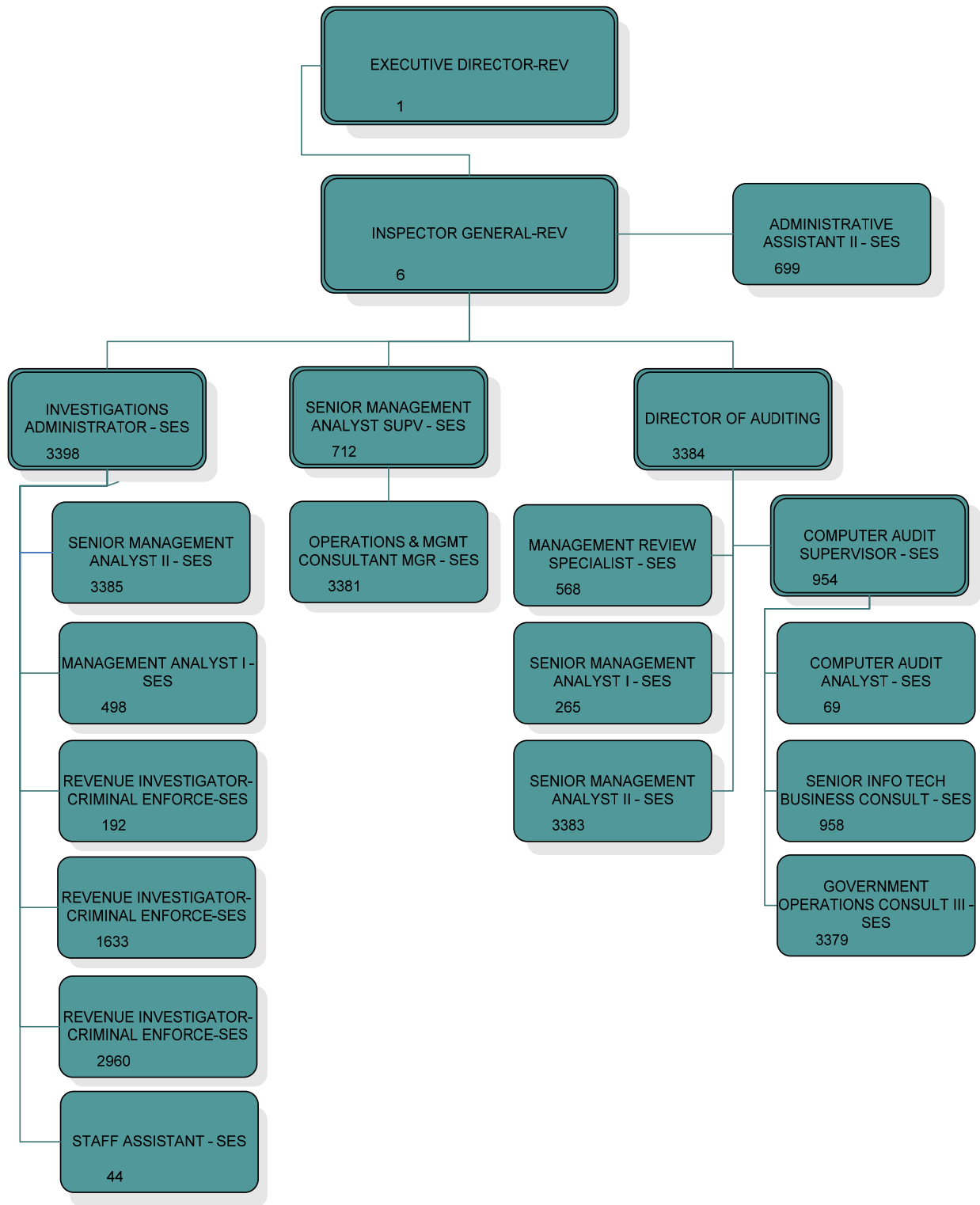
FY 2012/13



Table of Contents

Organizational Chart	<u>iii</u>
Background	<u>1</u>
Internal Audits Section	<u>5</u>
Internal Investigations Section	<u>17</u>
Special Projects Section	<u>23</u>
Appendix A	
Outstanding Corrective Actions for Prior Audit Reports	<u>31</u>
Appendix B	
Summary of Closed Internal Investigations for FY 2012/13	<u>42</u>

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 department 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, waste, and abuse; 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, waste, 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.

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.

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	2
Certified Information Systems Auditor – CISA	3
Certified Information Systems Security Professional – CISSP	2
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	2
Certified Inspector General Investigator – CIGI	4
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
- InfraGard

The OIG Corner

During FY 2012/13, the OIG continued publishing articles in Revenue's online internal news sources: *News You Can Use*, *Supervisor News You Can Use*, and *Department-Wide Key Communications*. The purpose of these articles, which are written by OIG staff, is to educate employees and management on the responsibilities and activities of the OIG in an open and non-intimidating manner. In addition, articles keep employees informed of important information concerning audits, investigations, discrimination, and other related subjects.

Articles published during FY 2012/13 were:

News You Can Use:

"Workplace Violence"

September 2012

Department-Wide Key Communication:

"Unauthorized Computer Use (Pornography)"

February 2013

Supervisor News You Can Use:

"OIG Corner: Translating 'Audit Speak' – Can You Say That In English?"

May 2013

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 direct 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*, 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:

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*.

- 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 Office of the Auditor General (OAG).

The IAS staff provides a variety of expertise to Revenue through consulting engagements. Many of the consulting engagements at Revenue involve participation on department 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

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

The *Standards* require audit staff to maintain their professional proficiency through continuing education and training. IAS staff accomplishes this by attending courses and/or conferences throughout the year. In the last year, staff has attended Association of Inspectors General local chapter meetings and training sessions; the Institute of Internal Auditors' local chapter meetings and training sessions; Association of Government Accountants' training; 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 department 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.

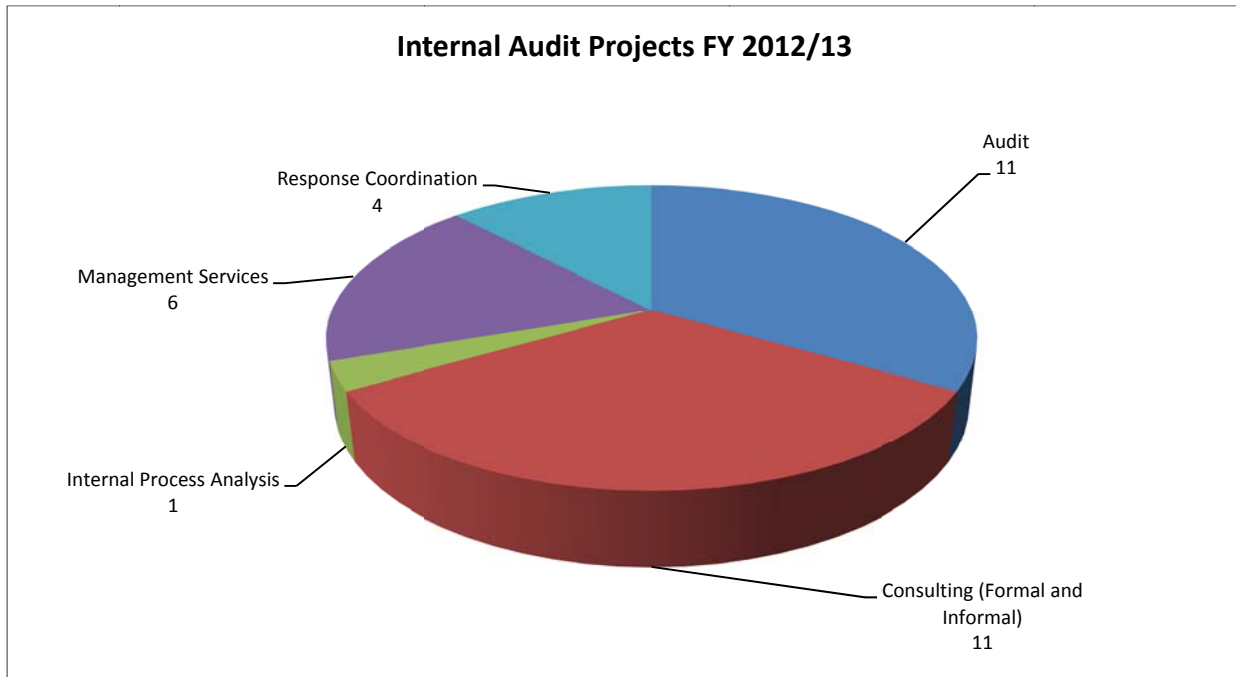
As required by section 20.055(5)(h), F.S., the OIG monitors the accomplishment of Revenue's responses and planned corrective actions to findings and recommendations made in reports issued by the OAG and the Office of Program Policy Analysis and Government Accountability (OPPAGA). The OIG is also required to provide a written report to Revenue's 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 submits a report no later than 18 months after the release of a report by OPPAGA to provide data and other information describing 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 timeframes.

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 FY2012/13. Detailed descriptions of the projects are included in the following section.



Assurance Engagements Conducted During FY 2012/13

During FY 2012/13, the IAS completed 11 audits, resulting in 13 reports. Below is a summary of the reports produced during the year.

Child Support Enforcement Program Income Verification Activity

The specific objectives of this audit were to:

- Determine if procedures developed by CSE to verify income for support orders and order modifications are in accordance with federal and state law.
- Determine if CSE is following best practices to verify income for support orders and order modifications.
- Determine if the steps taken by CSE to verify income for support orders and order modifications are effective.

The audit concluded:

- CSE procedures related to income verification are in accordance with federal and state laws.
- CSE is following best practices regarding verification of income for support orders and order modifications.

- The income verification activities performed by CSE are consistently performed and in conformance with requirements.

Information Services Program (ISP) Service Delivery – Continuity Process (Confidential)

The specific objectives of this audit were to:

- Determine whether ISP's continuity of mission critical systems that support mission essential functions complies with requirements applicable to Revenue's Continuity of Operations Plan.
- Determine whether an adequate continuity plan is in place to ensure timely and complete recovery of mission critical systems that support mission essential functions in Child Support Enforcement, General Tax Administration, Property Tax Oversight, Executive Direction and Support Services, and Information Services exists in conformance with Florida Statutes and Florida Administrative Code and if the plan is properly tested.

The audit concluded an adequate continuity plan is in place that complies with requirements applicable to the Revenue *Continuity of Operations Plan, Florida Statutes, and Florida Administrative Code* to recover mission critical systems that support mission essential functions, with some exceptions. Specific recommendations are deemed confidential in accordance with section 282.318(4)(f), Florida Statutes; as a result, the detailed recommendations are not included in this report.

Child Support Enforcement Program (CSE) Payment Processing – Fund Distribution (Non-Confidential)

The specific objectives of this audit were to:

- Determine if monitoring activities associated with the Fund Distribution Process are adequate and effective.
- Determine if guidance for the Fund Distribution Process is adequate.
- Determine if State Disbursement Unit (SDU) Contract Monitoring activities for distributions are adequate and effective.
- Determine if CSE data transmission controls related to disbursements ensure the timely, accurate, and complete processing of information between systems.
- Determine if the Complementary User Organization Controls identified by the service auditor are in place and operating effectively.
- Assess the reliability and validity of relevant performance measures reported to the Legislature.

The audit concluded that management has:

- Designed controls that are adequate for the Fund Distribution Business Process, with exceptions.

- Identified solutions to correct, or is already in the progress of correcting, many of the exceptions noted in the report.

The following improvements were recommended:

- The Department should consider reconciling the daily disbursement instruction file sent to the SDU with the actual bank disbursement records for each disbursement.
- The Department should designate, in accordance with the requirements of Amendment 11 to Contract No. C-3636, which SDU contractor's employees with access to the Department's information resources or facilities require a criminal background check. The Department should follow up to ensure that the criminal background checks are performed in accordance with Amendment 11.
- The Department should ensure that as additional SDU contractor's employees are granted access privileges to CSE Automated Management System (CAMS), a determination is made as to whether a criminal background check is required and follow-up be conducted to ensure that the criminal background checks are performed in accordance with Amendment 11.

Performance measures were validated in the FLORIDA system. Process performance measures could not be validated in the CAMS system because program staff was still working out a method to retrieve the necessary data from the CAMS system.

Child Support Enforcement Program (CSE) Payment Processing – Fund Distribution (Confidential)

The specific objectives of this audit were to:

- Determine if monitoring activities associated with the Fund Distribution Process are adequate and effective.
- Determine if guidance for the Fund Distribution Process is adequate.
- Determine if State Disbursement Unit (SDU) Contract Monitoring activities for distributions are adequate and effective.
- Determine if CSE data transmission controls related to disbursements ensure the timely, accurate, and complete processing of information between systems.
- Determine if the Complementary User Organization Controls identified by the service auditor are in place and operating effectively.
- Assess the reliability and validity of relevant performance measures reported to the Legislature.

Recommendations were made to improve specific information security issues that are deemed confidential in accordance with section 282.318(4)(f), Florida Statutes; as a result, the detailed recommendations are not included in this report.

General Tax Administration Return and Revenue Processing – Building L (Non-Confidential)

The specific objectives of this audit were to:

- Determine the adequacy and effectiveness of internal controls.
- Determine if expectations included in contracts, service level agreements (SLA) and other legal agreements between Building L and customers are met.

The audit concluded:

- Management has implemented adequate and effective internal controls for maintenance of procedures and for management of contracts between Building L and external customers. In addition, management has implemented internal controls for implementing Revenue's policies. However, the effectiveness of some internal control could be improved.
- Not all legal agreements between Building L and customers included the same language, nor did external customers approach elements of a contract (e.g., scope of work, customer responsibilities, security, etc.) the same way.
- None of the external customer agreements included performance measures in their contracts with Building L. Our observations and analysis did not reveal any discrepancies from expectations listed in the contracts.
- External customers confirmed contracts with Building L were renewed and that contract renewal was contingent upon satisfactory performance.

Specific recommendations were made to address the internal control weaknesses.

General Tax Administration Return and Revenue Processing – Building L (Confidential)

The specific objectives of this audit were to:

- Determine the adequacy and effectiveness of internal controls.
- Determine if expectations included in contracts, service level agreements (SLA) and other legal agreements between Building L and customers are met.

Recommendations were made to improve internal controls and specific information security issues that are deemed confidential in accordance with section 282.318(4)(f), Florida Statutes; as a result, the detailed recommendations are not included in this report.

Information Services Program Network Infrastructure Deployment Process (Confidential)

The specific objectives of this audit were to:

- Determine if responsibility and authority of network administration tasks are adequate and compliant with industry standards.
- Determine if physical security and inventory controls of network infrastructure equipment are adequate.

- Determine if the organization adequately establishes and documents mandatory configuration settings for information technology products employed within the network infrastructure.
- Determine if vulnerability scanning is adequately performed on network infrastructure equipment.

The audit concluded that management has designed controls that are adequate. Physical security and inventory controls of network infrastructure equipment are adequate.

Additional findings and recommendations were made regarding the security of information processed by the network, the reliability of the infrastructure, and the strength of existing controls that are deemed confidential in accordance with section 282.318(4)(f), Florida Statutes; therefore, the detailed recommendations are not included in this report.

Child Support Enforcement—Port Richey and Tampa Service Centers

The specific objective of this audit was to determine whether internal controls are adequate and effective.

The audit concluded the internal controls for the administrative functions within the service centers were generally adequate. The following observations and recommendations were made:

- CSE Port Richey and Tampa control activities related to property management are adequate and effective.
- CSE Port Richey and Tampa control activities related to physical security are adequate and effective.
- CSE Port Richey and Tampa management of selection packages could be improved.

Recommendations were made that Service Center management should obtain clarification regarding the retention of selection packages and should ensure that staff follows Revenue policies and procedures related to sending selection packages to the Office of Workforce Management.

Property Tax Oversight—Tampa Service Center

The specific objective of this audit was to determine whether internal controls are adequate and effective.

The audit concluded that management has implemented adequate and effective internal controls for property management and physical security.

Recommendations were made to improve specific information security issues that are deemed confidential in accordance with section 282.318(4)(f), Florida Statutes; as a result, the detailed recommendations are not included in this report.

Child Support Enforcement, General Tax Administration, and Property Tax Oversight— Tampa Service Center (Confidential)

The specific objective of this audit was to determine whether service center information practices comply with federal regulations, Florida Statutes, Florida Administrative Code, and Revenue policies.

The audit concluded the internal controls for the administrative functions within the service center were generally adequate, with some exceptions.

Recommendations were made to improve specific information security issues that are deemed confidential in accordance with section 282.318(4)(f), Florida Statutes; as a result, the detailed recommendations are not included in this report.

General Tax Administration—Port Richey and Tampa Service Centers

The specific objective of this audit was to determine whether internal controls are adequate and effective.

The audit concluded the internal controls for the administrative functions within the service centers were generally adequate.

- Control activities related to Remote Capture are adequate and effective.
- Control activities related to Cash Desk are adequate and effective.
- Control activities related to property management are adequate and effective.
- Control activities related to physical security are adequate and effective.
- Management of selection (hiring) packages could be improved.

Recommendations were made that Service Center management should obtain clarification regarding the retention of selection packages and should ensure that staff follows Revenue policies and procedures related to sending selection packages to the Office of Workforce Management.

Child Support Enforcement and General Tax Administration—Port Richey Service Center (Confidential)

The specific objective of this audit was to determine whether service center information practices comply with federal regulations, Florida Statutes, Florida Administrative Code, and Revenue policies.

The audit concluded that management has implemented adequate and effective internal controls for information security, with some exceptions.

Recommendations were made to improve specific information security issues that are deemed confidential in accordance with section 282.318(4)(f), Florida Statutes; as a result, the detailed recommendations are not included in this report.

General Tax Administration Program Chicago Service Center

The specific objectives of this audit were to:

- Determine whether service center information security practices comply with federal regulations, *Florida Statutes*, *Florida Administrative Code*, and Revenue policies regarding:
 - Software license management.
 - Unauthorized software on computers.
 - Antivirus software on computers.
 - Screen saver protection for workstations.
 - Laptops encryption.
 - Use of wireless devices.
- Determine whether internal controls are adequate and effective regarding:
 - Inventory and property management.
 - Physical security.
 - Hiring practices.
 - Purchasing activities.

The audit concluded the internal controls over the administrative functions within the service centers were generally adequate. However, the following improvements were recommended:

- Established procedures for processing selection packets should be followed.
- Printing supply purchases could be reduced by utilizing the high capacity printers instead of individual printers.
- Travel costs could be reduced by utilizing available technologies for remote communication.

Additional recommendations were made to improve specific information security issues that are deemed confidential in accordance with section 282.318(4)(f), Florida Statutes; as a result, the detailed recommendations are not included in this report.

Consulting Engagements Conducted During FY 2012/13

During FY 2012/13, IAS completed 11 consulting engagements. IAS staff also participated on teams that addressed agency-wide topics such as computer security and contract management.

IAS assisted the OIG's investigations staff by performing forensic reviews of computers, pulling information from Revenue's information systems and providing analyses of data. IAS staff performed five forensic reviews of computers and assisted in a number of other internal investigations during FY 2012/13.

Below is a summary of consulting activities that resulted in a management letter or final report.

Follow-Up on Corrective Action Plans as of June 30, 2012

The purpose of this review was to follow up on the program assertions for the corrective action plans as of June 30, 2012. A summary report was provided to the Executive Director indicating there were 64 open findings and 19 findings verified by OIG staff as closed during the period.

Six-Month Follow-Up of Auditor General CAMS IT Audit

The purpose of this review was to provide a six-month status update, as required by statute, on corrective actions taken in response to the Auditor General's Report No. 2012-142.

Six-Month Follow-Up of Auditor General Federal Awards/Financial Statements Audit

The purpose of this review was to provide a six-month status update, as required by statute, on corrective actions taken in response to the Auditor General's Report No. 2013-034.

Six-Month Follow-Up of Auditor General Information Technology Audit of SUNTAX and IMS Systems

The purpose of this review was to provide a six-month status update, as required by statute, on corrective actions taken in response to the Auditor General's Report No. 2011-192.

Six-Month Follow-Up of Auditor General Operational Audit of Administration of Insurance Premium Tax

The purpose of this review was to provide a six-month status update, as required by statute, on corrective actions taken in response to the Auditor General's Report No. 2011-194.

Follow-Up on Corrective Action Plans as of December 31, 2012

The purpose of this engagement was to follow up on the program assertions for the corrective action plans as of December 31, 2012. A summary report was provided to the Executive Director indicating there were 73 open findings and 30 findings verified by OIG staff as closed during the period. See [Appendix A](#) for a list of the Outstanding Corrective Actions for Prior Audit Reports.

Information Services Program (ISP) ISO 20000 Audit Assistance

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

Validity and Reliability Review of Agency Submitted Legislative Budget Request (LBR)/Long-Range Program Plan (LRPP) Performance Measures

The purpose of this engagement was to review the validity and reliability of performance measures submitted by the agency for the LBR/LRPP process.

Microsoft Proofing Tools

Staff researched the Microsoft Office 2010 Help Improve Proofing Tools feature, which collects data such as additions to the custom dictionary from the use of the proofing tools feature, and forwards this information to Microsoft. The application is also collecting information about the

writer's style and formatting that may help Microsoft to add new features to assist users. Although the application does not appear to target specific user information, a compromise to the integrity of the Revenue information security system may be occurring.

General Tax Administration Atlanta Service Center

Staff researched a reimbursement request by a former Revenue employee and the appropriate procedure associated with the payment of invoices to a contracted service provider.

Child Support Enforcement Reconciliation Scope of Work Review

Staff reviewed the State Distribution Unit Reconciliation Scope of Work that is being developed for the upcoming Invitation to Negotiate.

Other IAS Services

IAS provides services related to internal process analysis (one project), management services (six projects), and response coordination (four projects).

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 attend program executive briefings, monitor the programs' corrective action plans to address audit findings and recommendations, coordinate external audits conducted by other entities, and coordinate Revenue's responses to those audits.

The IAS also provided the following notable management services:

- Coordinated Revenue's participation in the Chief Inspector General's enterprise engagement concerning background screenings for prospective and current employees.
- Completed a review in response to a request from the Department of Highway Safety and Motor Vehicles (HSMV) for an attestation related to the Data Exchange Memorandum of Understanding between HSMV and Revenue.

Other IAS Accomplishments During FY 2012/13

Two IAS staff members obtained the following professional designation:

- Internal Auditor Certification in Information Technology Service Management (ITSM) according to ISO/IEC 20000-1:2011.

Internal Investigations Section

The Internal Investigations Section (IIS) is responsible for conducting internal investigations to resolve allegations of violations of department 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 and provides assistance to local, state, and federal law enforcement agencies on cases related to possible criminal violations or activities.

Each complaint received by the OIG is preliminarily reviewed by IIS staff. The preliminary review process is used 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.

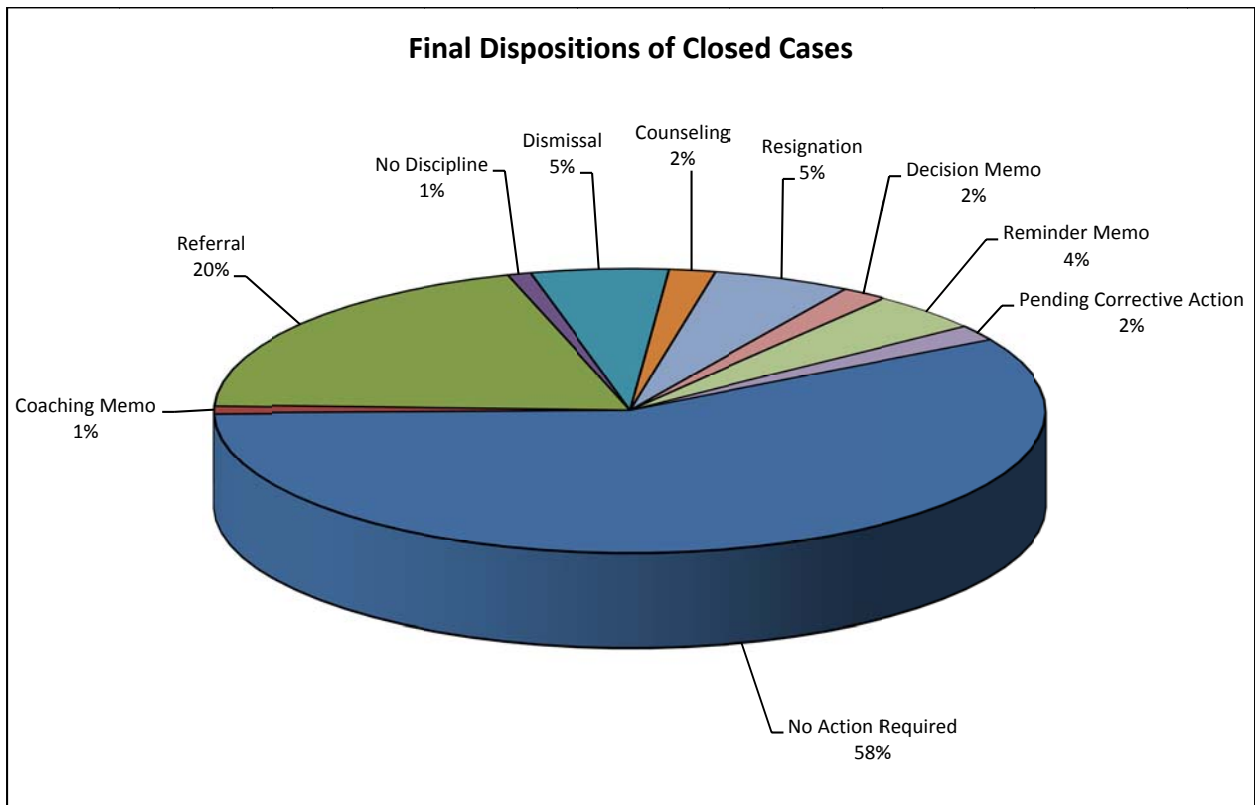
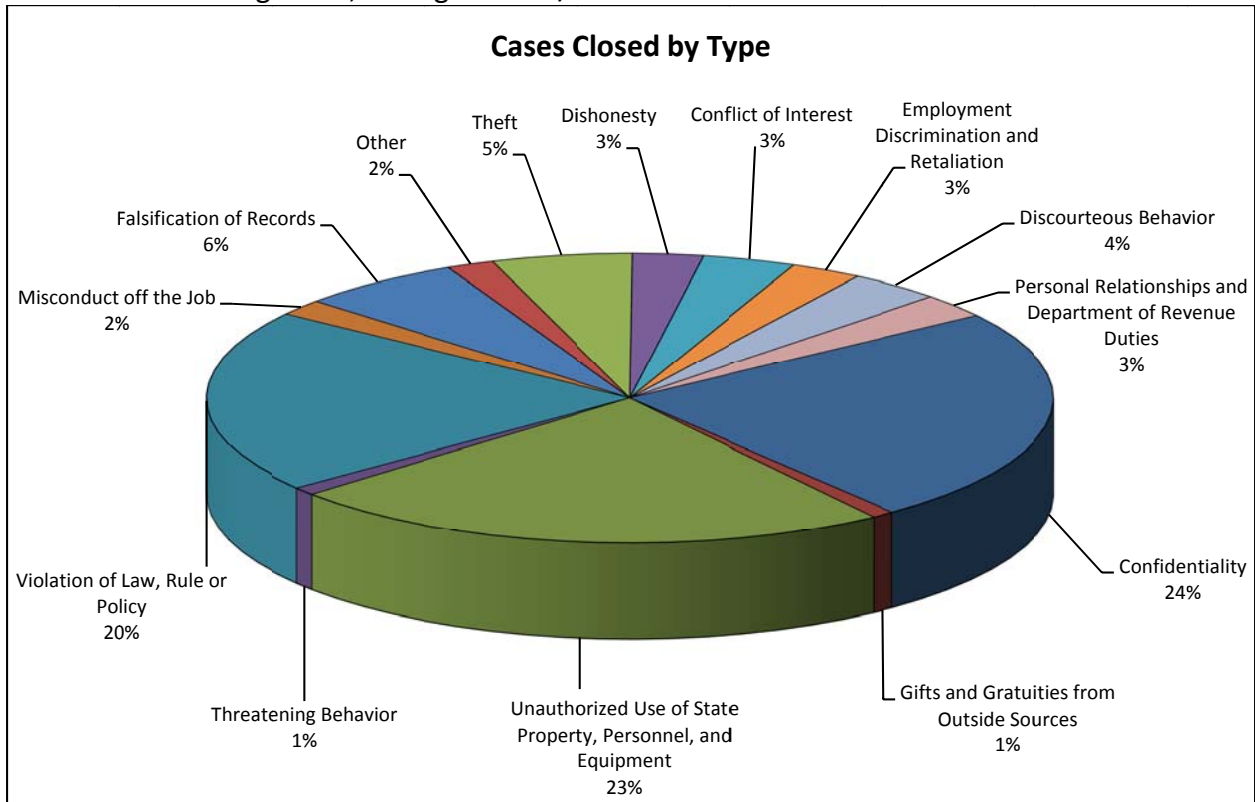
Internal Investigations Section Accomplishments During FY 2012/13

- IIS earned accreditation through the Commission for Florida Law Enforcement Accreditation (CFA). This involved an on-site assessment by CFA to ensure processes, policies, and procedures are in place to meet the 42 standards mandated by the Commission.
- Updated the *IIS Policies and Procedures Manual*.
- Reduced travel costs for investigations by conducting some investigatory interviews remotely through a secured Internet video conferencing system.
- One staff member successfully completed the Certified Inspector General Investigator training course. After receiving several hours of classroom instruction, the staff member passed a written examination in the core competencies of the investigative function within the Inspector General discipline to attain certification as a Certified Inspector General Investigator (CIGI).



The Office of Inspector General Internal Investigation Section received accreditation from the Commission for Florida Law Enforcement Accreditation (CFA) on June 27, 2013. The accreditation program for Florida agencies' Offices of Inspectors General was implemented by CFA in October 2007. The program is designed to ensure professional standards and enhance the quality of investigations.

The following charts reflect the types and outcomes of cases closed, including preliminary reviews and investigations, during FY 2012/13.



Investigation Summaries for FY 2012/13

A number of significant investigations were conducted during FY 2012/13. The following are highlights of some of these cases:

Falsification of Records, Unauthorized Use of State Property, Personnel and Equipment, and Violation of Law, Rule or Policy

The OIG received allegations from management that an employee may be spending an excessive amount of time on the Internet for non-work related purposes. Furthermore, sexually explicit images were found on a computer previously assigned to the employee. In addition, the Discrimination Intake Officer received information that the employee was making sexually inappropriate comments to co-workers. The OIG investigation revealed that the employee accessed and saved numerous inappropriate images to his Revenue computer, spent excessive work time using his assigned Revenue computer for non-work related activities, made comments to co-workers that were inappropriate for the workplace, and falsified his People First timesheets by inflating the time recorded under the project codes to account for the excessive work time spent on personal use of the Internet for approximately the past one and a half to two years. The employee was dismissed from his position with Revenue.

Employment Discrimination and Confidentiality

The OIG received information from the Discrimination Intake Officer that a manager may have subjected a female subordinate to unwelcome and offensive physical and verbal behavior of a sexual nature on numerous occasions. During the course of the investigation, information was also obtained that the manager may have accessed and/or viewed the subordinate's child support case for unauthorized purposes. The OIG's investigation revealed that there was insufficient evidence that the manager violated Revenue's *Non-Discrimination Policy and Complaint Procedures*; however, the investigation revealed that there was sufficient information to support a finding that the manager engaged in inappropriate behavior for the workplace. Additionally, the OIG's investigation supported a finding that the manager accessed and viewed the child support case of his subordinate for unauthorized purposes. During the investigation, the manager retired from his position with Revenue.

Unauthorized Use of State Property, Personnel, and Equipment, and Violation of Law, Rule, Regulation or Policy

The OIG received information from the Information Services Program (ISP), Policy and Monitoring Process, that a manager may have been browsing inappropriate sites using his assigned Revenue computer. During an OIG interview, the manager admitted that he saved images to his Revenue computer from the Internet and that the images he saved may be considered inappropriate for the workplace. The investigation supported a finding that the

employee accessed, viewed, and saved inappropriate images. The manager resigned from his position with Revenue.

Confidentiality and Conduct Unbecoming a Public Employee

The OIG received a complaint from a general counsel for a major corporation alleging that a Revenue employee disclosed her Revenue assignment to an employee of the corporation because she was dissatisfied with the outcome of a personal business transaction with the corporation. The investigation supported a finding that the employee disclosed the existence of the Revenue assignment to unauthorized individuals and made statements suggesting she would consider her dissatisfaction with her personal business transaction when performing her Revenue assignment. The employee was issued a reminder memo.

Confidentiality and Unauthorized Use of State Property, Personnel, and Equipment

The OIG received information that an employee may be accessing her own personal child support case information for unauthorized purposes. During the course of the investigation, it was discovered that the employee may also have been accessing the child support case information for other family members for non-business related purposes. Information obtained during the investigation, as well as the employee's admission, substantiated findings that the employee accessed and viewed confidential child support information for her own child support cases and those of family members for unauthorized purposes. The employee was dismissed from her position with Revenue.

Theft

The OIG received an allegation that an individual owing child support, while visiting the CSE office, was asked by an employee to place a \$550 cash payment inside a magazine the employee had in his possession. The OIG referred the complaint to the Florida Department of Law Enforcement (FDLE). The referral reflected that the employee allegedly asked for and received \$550 cash from the individual owing support that the individual believed was intended to be credited to his child support; however, the cash payment was never credited to the individual's child support account. The OIG provided FDLE with two supplemental referrals based upon additional complaints received from other individuals owing child support about the same Revenue employee accepting cash and not crediting their accounts. The employee resigned from his Revenue position and was arrested and charged with organized fraud.

Theft and Misconduct

The OIG received information that an employee may have taken two money orders given to her by an individual owing support and used them to pay personal expenses. The OIG received a handwritten letter from the individual owing support, along with copies of two money orders, which he stated were intended to be credited to his past due “cost payment” balance but never were. The investigation revealed that the Revenue employee used the money orders to pay for her water bill and past due childcare. The employee was dismissed from her position based on an earlier investigation conducted on violations of Revenue’s Standards of Conduct. The allegations of the theft were referred to a local law enforcement agency for possible criminal investigation.

See [Appendix B](#) for the Summary of Closed Cases for FY 2012/13, which includes 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, including assaults and threats from external customers, domestic violence affecting the workplace, and incidents of violent behavior between employees.
- Follow-up reviews of employees' reports of current arrests.
- Discrimination and sexual harassment complaint intake.
- Fraud prevention and response.

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

Special Projects Section Accomplishments During FY 2012/13

- Worked with ISP and the Office of General Counsel (OGC) to create a condensed security awareness training module for new employees and contractors' employees.
- Reduced the number of days to close a current arrest review from 74 to 30 days.
- Assisted the Internal Investigations Section in meeting requirements to attain accreditation from the Florida Commission on Law Enforcement Accreditation.
- Successfully and seamlessly transitioned the discrimination complaint Intake process from the OIG to the Office of Workforce Management.
- Initiated the establishment of a fraud program for Revenue, including drafting of a proposed agency-wide policy specifically addressing fraud prevention and response.

Workplace Violence

Revenue's security policies and procedures emphasize protecting employees from all forms of workplace violence. 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 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.

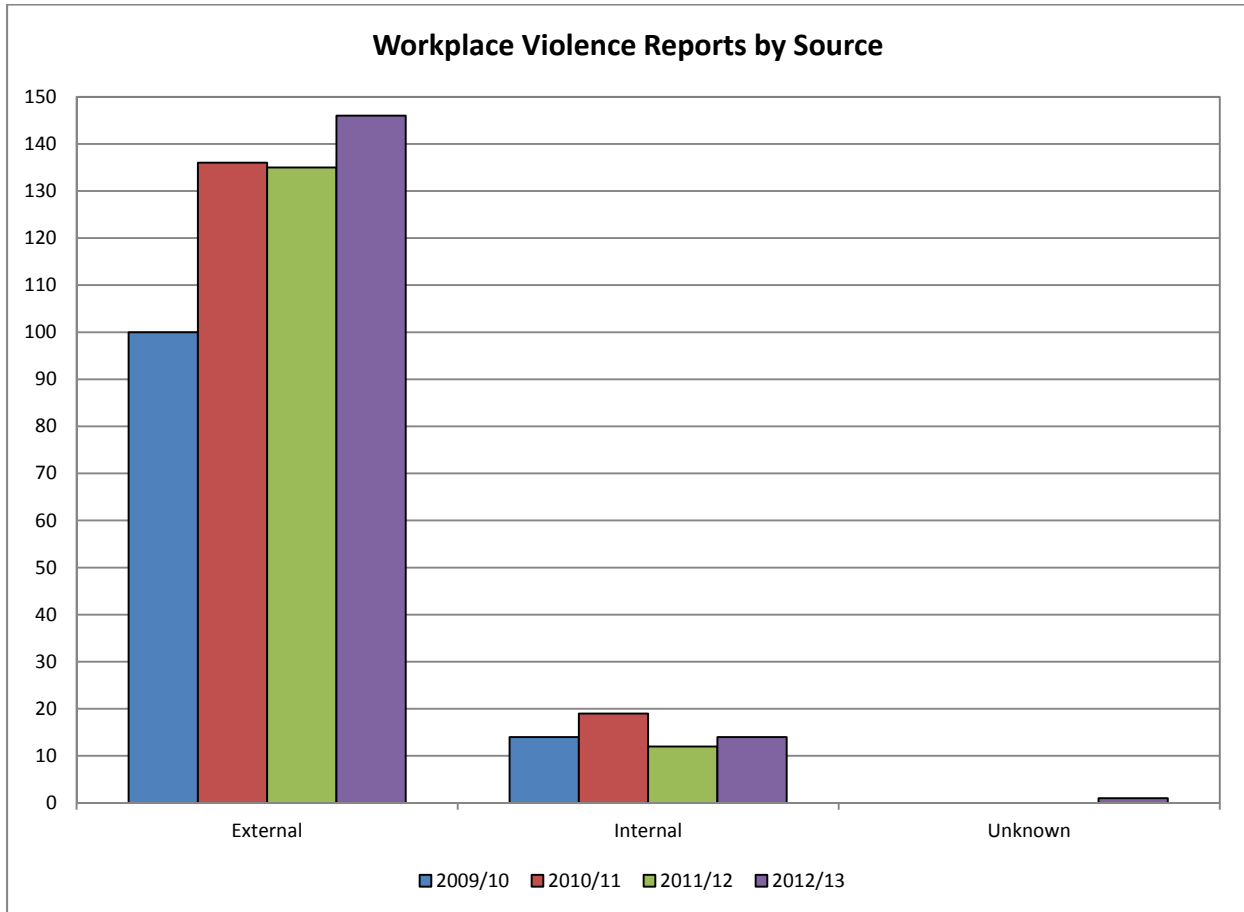
When it is determined that a potentially violent person may be associated with a tax account or child support case, a Potentially Dangerous Contact (PDC) indicator is placed on applicable primary databases used within the operating programs of Revenue. This indicator flag serves notice to an employee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

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 Executive Direction and Support Services Program. The WPV Team works cooperatively to determine and advise management of the best response to reported incidents. The WPV Team's recommendation may include disciplinary action, counseling, mitigation, or referral to the Employee Assistance Program (EAP). The WPV Team may also request an internal investigation if facts of the incident cannot easily be determined.

Domestic violence affecting the workplace is a primary concern for any agency or business. Domestic violence could 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 reason to believe the respondent may come to the workplace. The SPS works with

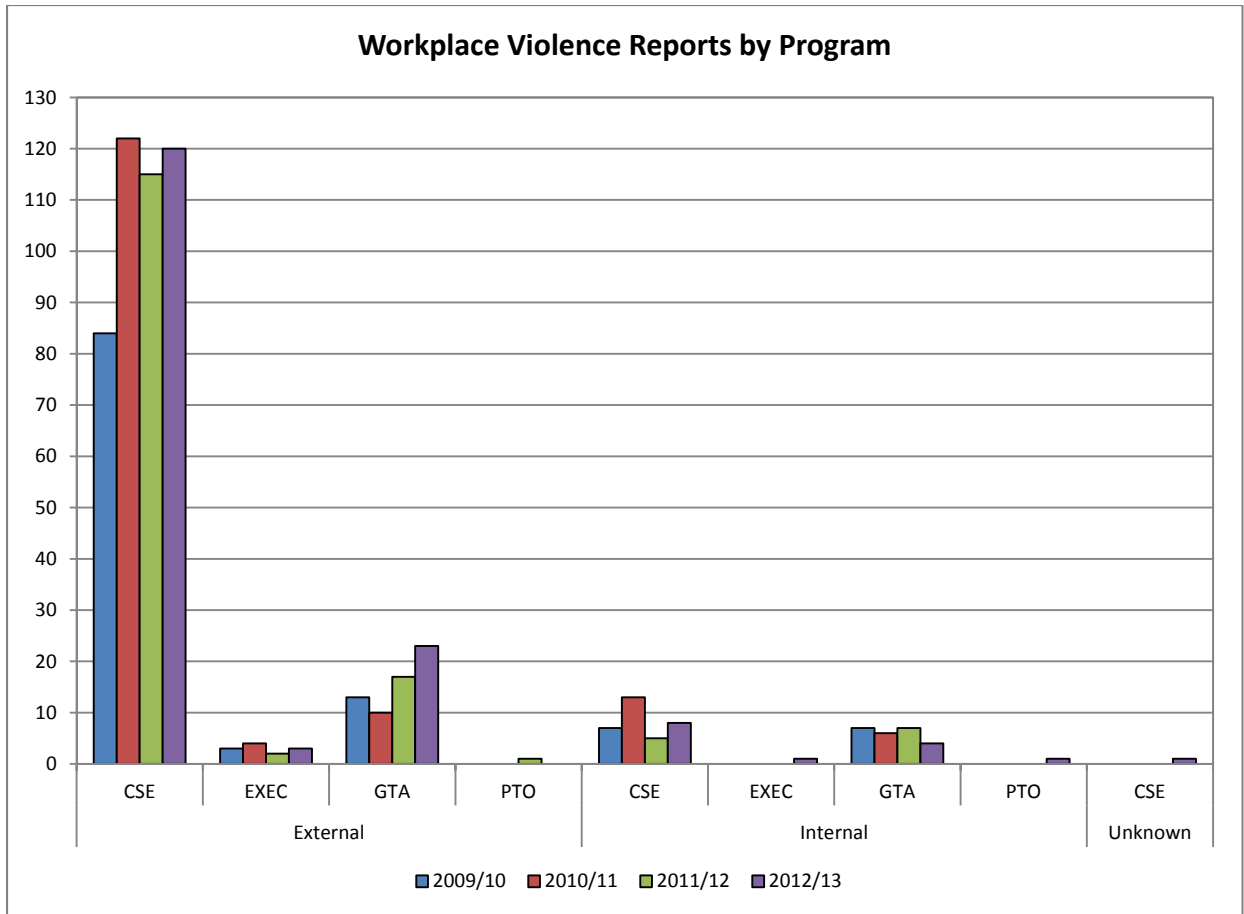
appropriate management to take necessary action to protect victims of domestic violence in the workplace, as well as to help ensure the safety of the victim's co-workers. The WPV Team may be convened to address more serious incidents of domestic violence affecting the workplace.

The following chart reflects the total number of workplace violence incidents received for the past four years by source:



A total of 161 reports of actual or potential workplace violence were received during FY 2012/13, a slight increase from the 147 incidents reported during the previous fiscal year. Fourteen of these incidents involved a Revenue employee as the perpetrator and the source of one reported incident was unknown.

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



During FY 2012/13, Child Support Enforcement (CSE) reported 120 incidents from external sources, 8 incidents from internal sources, and 1 incident from an unknown source; General Tax Administration (GTA) reported 23 incidents from external sources and 4 incidents from internal sources; Executive Direction and Support (EXEC) reported 3 incidents from external sources and 1 incident from an internal source; and Property Tax Oversight (PTO) reported 1 incident from an internal source. The Information Services Program (ISP) reported no incidents 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

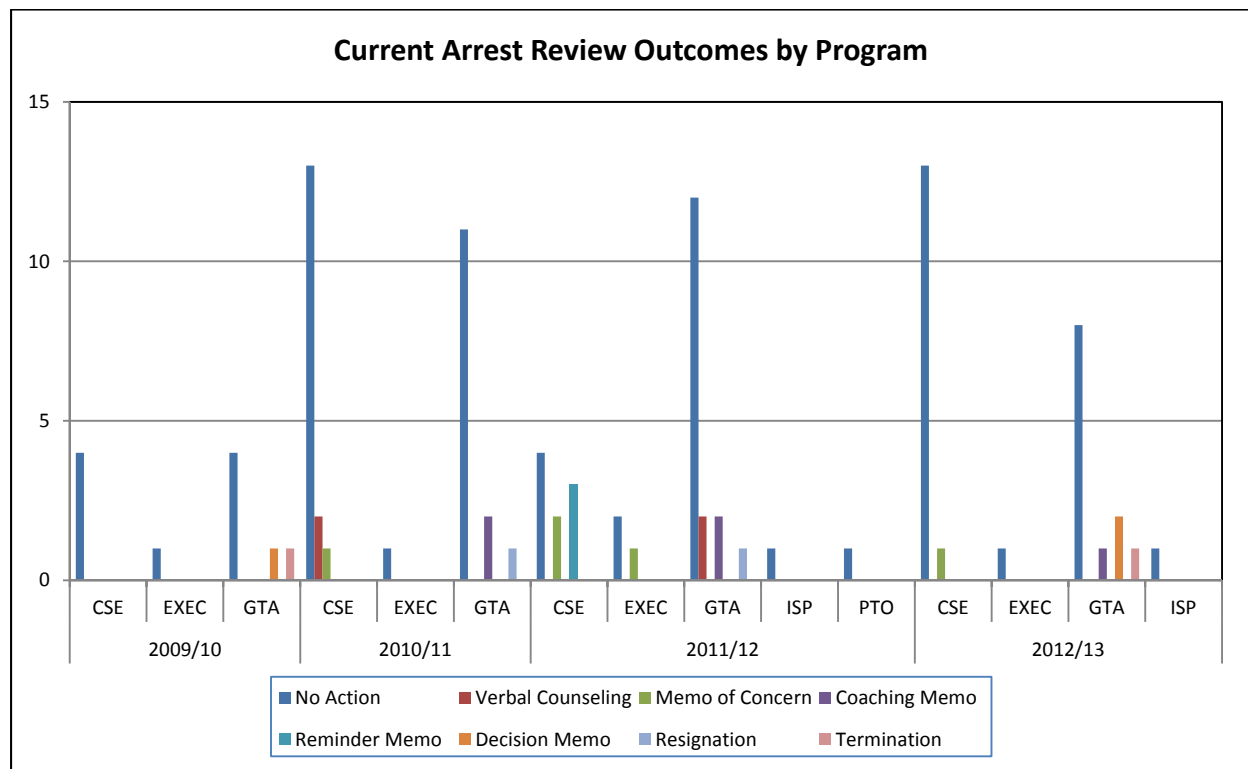
The SPS is responsible for receiving and following up on reports of current employees who are arrested or charged with criminal offenses. Revenue's *Standards of Conduct* require that employees timely report the following events to the OIG:

- 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-five current arrest reports were received and Twenty-eight current arrest follow-up review cases were closed during the fiscal year. The following chart reflects the outcome of current arrest follow-up reviews by program for the past four years:



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

Discrimination Complaint Intake

Revenue is committed to providing a positive work environment for all employees and strives to ensure that each employee is able to work in an environment that is free from all forms of discrimination. Revenue's *Non-Discrimination Policy and Complaint Procedures* cover all forms of employment discrimination prohibited by the Florida Civil Rights Act and Title VII of the federal Civil Rights Act, including sexual harassment and retaliation. The policy includes examples and sets forth the rights and responsibilities of Revenue employees and managers.

Any employee may seek relief from discrimination inside the agency and/or outside of the agency through the Florida Commission on Human Relations (FCHR) or the Equal Employment Opportunity Commission (EEOC), without fear of retaliation. Additionally, Revenue's *Non-Discrimination Policy* requires that any supervisory employee must promptly report to the Discrimination Intake Officer any observations, complaints, or reports of alleged discriminatory behavior involving any employee he or she supervises, or involving any employee supervised by another. A supervisory employee who fails to promptly report alleged discriminatory behavior to the Discrimination Intake Officer may be subject to corrective action, up to and including dismissal.

Intake and preliminary review of discrimination complaints was transferred from the OIG to the Office of Workforce Management (OWM) in March 2013. Prior to that time, intake and preliminary review of discrimination complaints was assigned to the SPS. The Operations and Management Consultant Manager in the SPS served as the Discrimination Intake Officer for Revenue until the transfer of the intake process was completed. The Discrimination Intake Officer is responsible for gathering enough information during initial review to make a determination of the next appropriate action. The next action may include but is not be limited to referral to IIS, program management, other entities, or, in some cases, no further action may be required. To facilitate a clean transfer, it was determined that reviews of complaints of discrimination that were received in the OIG prior to the transfer of the process to OWM would be completed by SPS staff.

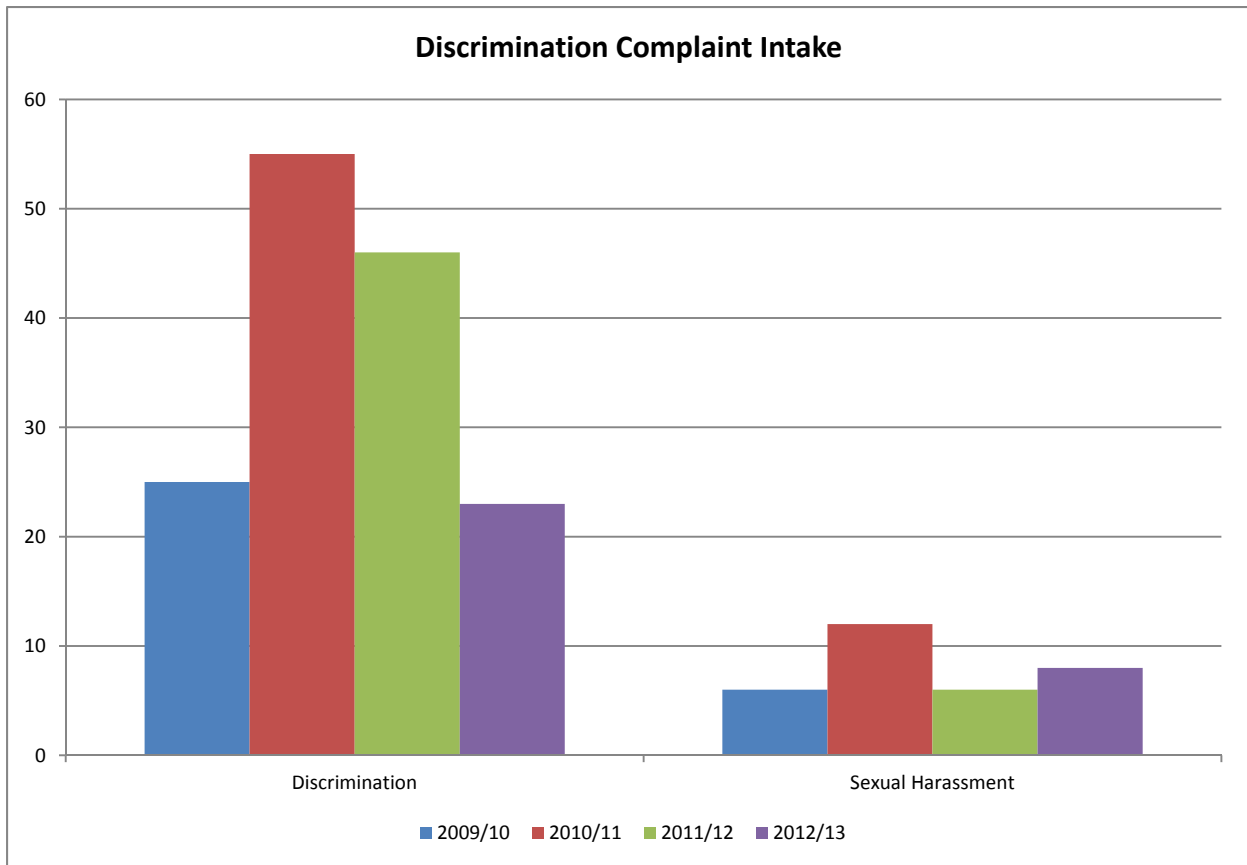
If the Discrimination Intake Officer's review of a complaint or allegation of discrimination determines the case possesses the necessary prima facie elements, if proven factual, to support a formal charge of discrimination through the FCHR or EEOC, the case is referred to the Internal Investigations Section for investigation. Upon completion of the internal investigation, each allegation of discrimination that is referred to IIS is reviewed by a Discrimination Review Board, which is made up of executive level managers responsible for making a final "cause" or "no-cause" determination and deciding the appropriate corrective action, up to and including dismissal.

If the Discrimination Intake Officer's review of a complaint or allegation of discrimination determines that the allegations or complaints are insufficient to constitute discrimination, but require a manager to address inappropriate workplace behavior in accordance with Revenue's *Standards of Conduct*, the case is referred to the appropriate program

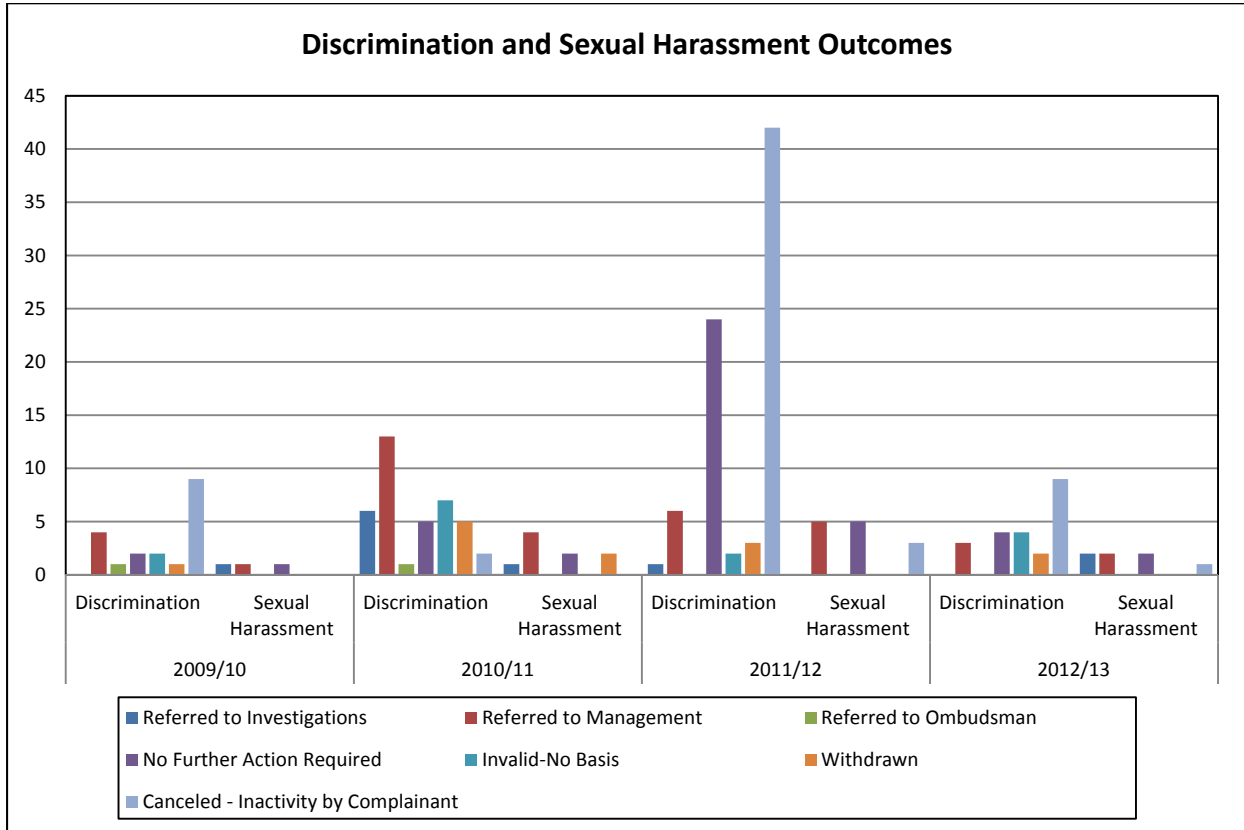
management. When referrals to management are made, the Discrimination Intake Officer may make recommendations to include training and/or other actions that are sufficient to prevent inappropriate behavior from re-occurring. Managers are responsible for working with OWM to coordinate any recommended training or to determine and initiate other appropriate corrective action when necessary.

While sexual harassment is a form of sex discrimination, to provide a more focused review, allegations involving only sexual harassment have been reported separately from other forms of discrimination in the following charts.

The following chart reflects internal complaints of discrimination received for the past four years. During FY 2012/13, prior to transfer of the discrimination intake process to OWM, 31 reports of alleged discrimination were received in the OIG, eight of which were complaints or allegations of sexual harassment.



The following chart reflects the outcomes of reviews of complaints or allegations of discrimination for the past four fiscal years. During FY 2012/13, the Discrimination Intake Officer completed review of 29 discrimination complaints, seven of which were reports of sexual harassment allegations.



During FY 2012/13, two employees who participated in Revenue’s internal discrimination complaint intake and review process also filed an external charge of discrimination with the EEOC or the FCHR.

Appendix A

Outstanding Corrective Actions for Prior Audit Reports

IAS Engagements Outstanding Corrective Actions as of 6/30/13		
Project No.	Audit Name	Recommendation
2007-0053	ISP Web Applications Development	Confidential
2007-0053	ISP Web Applications Development	Confidential
2007-0067	Internet Tax Applications	Confidential
2007-0067	Internet Tax Applications	Confidential
2008-0115-A	ISP Security Monitoring and Response	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	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	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	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.

IAS Engagements Outstanding Corrective Actions as of 6/30/13		
Project No.	Audit Name	Recommendation
2009-0107 A	Contract Management Process	We also recommend the contract manager's supervisors complete the contract monitoring training.
2009-0107 A	Contract Management Process	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	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	We recommend ISP request assistance through the SLB in gaining program participation and representation in the Requirements Process.
2009-0113-A	ISP/Agency Application Management-Requirements	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	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	We recommend that GTA management develop an oversight program to review cash received at GTA service centers to ensure that receipts are timely deposited in the State Treasury in compliance with section 116.01, F.S.

IAS Engagements Outstanding Corrective Actions as of 6/30/13		
Project No.	Audit Name	Recommendation
2009-0116 A	GTA Cash Handling	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.
2010-0110	General Tax Administration Receivables Write-Offs (DL-17)	We recommend GTA management review SAP specifications and ensure that an audit trail is maintained in the detailed record screen in SAP for all collection activities and enforcement actions, particularly those of issued and satisfied warrants documenting all of the filing information such as the county, the book and page number of the COC records, dates, and any other information necessary to provide management with adequate information about the filing of tax warrants and identifying the Revenue employee who issued the warrant and the warrant satisfaction, if applicable.
2010-0110	General Tax Administration Receivables Write-Offs (DL-17)	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)	We recommend that Revenue accrue and prepare an allowance for all types of taxes collected by Revenue, with the exception of unemployment tax, which is recorded by the Agency for Workforce Innovation (AWI).
2010-0113 A	Contract Compliance and Management - CSE DNA Contract	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	Confidential

IAS Engagements Outstanding Corrective Actions as of 6/30/13		
Project No.	Audit Name	Recommendation
2010-0115-A	ISP Telecom VOIP	Confidential
2010-0115-A	ISP Telecom VOIP	Confidential
2010-0115-A	ISP Telecom VOIP	Confidential
2010-0115-A	ISP Telecom VOIP	Confidential
2010-0115-A	ISP Telecom VOIP	Confidential
2010-0115-A	ISP Telecom VOIP	Confidential
2010-0115-A	ISP Telecom VOIP	Confidential
2010-0115-A	ISP Telecom VOIP	Confidential
2010-0115-A	ISP Telecom VOIP	Confidential
2010-0115-A	ISP Telecom VOIP	Confidential
2010-0115-A	ISP Telecom VOIP	Confidential
2010-0119-A2	GTA Dallas Out-Of-State Service Center-Confidential	Confidential
2010-0119-A2	GTA Dallas Out-Of-State Service Center-Confidential	Confidential
2010-0120-A1	GTA Pittsburgh Out-Of- State Service Center	We recommend the GTA Pittsburgh Service Center Manager ensure that supervisory staffs receive additional instruction or training on establishing critical job tasks, development of corresponding performance measures and standards for the job tasks, and the numeric scoring of evaluations.
2010-0120-A1	GTA Pittsburgh Out-Of- State Service Center	We also recommend the GTA Pittsburgh Service Center Manager monitor EE&Ds to ensure EE&Ds (1) contain critical job tasks with appropriate measurements and standards for those job tasks, and (2) are correctly scored.
2010-0120-A1	GTA Pittsburgh Out-Of- State Service Center	We recommend the EE&D reviewer ensure the accuracy of each EE&D reviewed and that the process steps are carried out as designed.

IAS Engagements Outstanding Corrective Actions as of 6/30/13		
Project No.	Audit Name	Recommendation
2010-0120-A1	GTA Pittsburgh Out-Of-State Service Center	We recommend the GTA Pittsburgh Service Center Manager ensure that supervisory staff routinely review mandatory training requirements through LMS and make sure that their employees complete all required mandatory training and complete it timely.
2010-0120-A2	GTA Pittsburgh Out-Of-State Service Center-Confidential	Confidential
2010-0120-A2	GTA Pittsburgh Out-Of-State Service Center-Confidential	Confidential
2010-0121-A1	GTA In-State Service Centers - Miami, Coral Springs, West Palm Beach	(Miami North) We recommend the GTA Miami South, Miami North, Coral Springs and West Palm Beach Service Center supervisory staffs establish appropriate critical job tasks, performance measures, and standards as each new evaluation is opened during the next year. Supervisory staff should ensure that critical job tasks in position descriptions are in line with critical job tasks included on EE&Ds.
2010-0121-A1	GTA In-State Service Centers - Miami, Coral Springs, West Palm Beach	(Miami South) We recommend the GTA Miami South, Miami North, Coral Springs and West Palm Beach Service Center supervisory staffs establish appropriate critical job tasks, performance measures, and standards as each new evaluation is opened during the next year. Supervisory staff should ensure that critical job tasks in position descriptions are in line with critical job tasks included on EE&Ds.
2010-0121-A1	GTA In-State Service Centers - Miami, Coral Springs, West Palm Beach	(Coral Springs) We recommend the GTA Miami South, Miami North, Coral Springs and West Palm Beach Service Center supervisory staffs establish appropriate critical job tasks, performance measures, and standards as each new evaluation is opened during the next year. Supervisory staff should ensure that critical job tasks in position descriptions are in line with critical job tasks included on EE&Ds.

IAS Engagements Outstanding Corrective Actions as of 6/30/13		
Project No.	Audit Name	Recommendation
2010-0121-A1	GTA In-State Service Centers - Miami, Coral Springs, West Palm Beach	(West Palm Beach) We recommend the GTA Miami South, Miami North, Coral Springs and West Palm Beach Service Center supervisory staffs establish appropriate critical job tasks, performance measures, and standards as each new evaluation is opened during the next year. Supervisory staff should ensure that critical job tasks in position descriptions are in line with critical job tasks included on EE&Ds.
2010-0121-A1	GTA In-State Service Centers - Miami, Coral Springs, West Palm Beach	(Miami North) We also recommend the GTA Miami South, Miami North, Coral Springs and West Palm Beach Service Center Managers monitor EE&D Plans to ensure EE&Ds contain critical job tasks with appropriate measurements and standards for those job tasks and EE&D policy provisions are followed.
2010-0121-A1	GTA In-State Service Centers - Miami, Coral Springs, West Palm Beach	(Miami South) We also recommend the GTA Miami South, Miami North, Coral Springs and West Palm Beach Service Center Managers monitor EE&D Plans to ensure EE&Ds contain critical job tasks with appropriate measurements and standards for those job tasks and EE&D policy provisions are followed.
2010-0121-A1	GTA In-State Service Centers - Miami, Coral Springs, West Palm Beach	(Coral Springs) We also recommend the GTA Miami South, Miami North, Coral Springs and West Palm Beach Service Center Managers monitor EE&D Plans to ensure EE&Ds contain critical job tasks with appropriate measurements and standards for those job tasks and EE&D policy provisions are followed.
2010-0121-A1	GTA In-State Service Centers - Miami, Coral Springs, West Palm Beach	(West Palm Beach) We also recommend the GTA Miami South, Miami North, Coral Springs and West Palm Beach Service Center Managers monitor EE&D Plans to ensure EE&Ds contain critical job tasks with appropriate measurements and standards for those job tasks and EE&D policy provisions are followed.

IAS Engagements Outstanding Corrective Actions as of 6/30/13		
Project No.	Audit Name	Recommendation
2010-0121-A1	GTA In-State Service Centers - Miami, Coral Springs, West Palm Beach	(Miami North) We recommend the GTA Miami South, Miami North, Coral Springs and West Palm Beach Service Center Managers ensure that supervisory staff routinely review mandatory training requirements through LMS and make sure their employees complete all required mandatory training and complete it timely.
2010-0121-A1	GTA In-State Service Centers - Miami, Coral Springs, West Palm Beach	(Miami South) We recommend the GTA Miami South, Miami North, Coral Springs and West Palm Beach Service Center Managers ensure that supervisory staff routinely review mandatory training requirements through LMS and make sure their employees complete all required mandatory training and complete it timely.
2010-0121-A1	GTA In-State Service Centers - Miami, Coral Springs, West Palm Beach	(Coral Springs) We recommend the GTA Miami South, Miami North, Coral Springs and West Palm Beach Service Center Managers ensure that supervisory staff routinely review mandatory training requirements through LMS and make sure their employees complete all required mandatory training and complete it timely.
2010-0121-A1	GTA In-State Service Centers - Miami, Coral Springs, West Palm Beach	(West Palm Beach) We recommend the GTA Miami South, Miami North, Coral Springs and West Palm Beach Service Center Managers ensure that supervisory staff routinely review mandatory training requirements through LMS and make sure their employees complete all required mandatory training and complete it timely.
2010-0121-A1	GTA In-State Service Centers - Miami, Coral Springs, West Palm Beach	(Miami North) We recommend the GTA Miami South, Miami North, Coral Springs and West Palm Beach Service Center Managers ensure that the telecommuting/virtual office forms for participation in the Alternate Work Program are completed and approved timely and participants complete the training required by the policy.

IAS Engagements Outstanding Corrective Actions as of 6/30/13		
Project No.	Audit Name	Recommendation
2010-0121-A1	GTA In-State Service Centers - Miami, Coral Springs, West Palm Beach	(Miami South) We recommend the GTA Miami South, Miami North, Coral Springs and West Palm Beach Service Center Managers ensure that the telecommuting/virtual office forms for participation in the Alternate Work Program are completed and approved timely and participants complete the training required by the policy.
2010-0121-A1	GTA In-State Service Centers - Miami, Coral Springs, West Palm Beach	(Coral Springs) We recommend the GTA Miami South, Miami North, Coral Springs and West Palm Beach Service Center Managers ensure that the telecommuting/virtual office forms for participation in the Alternate Work Program are completed and approved timely and participants complete the training required by the policy.
2010-0121-A1	GTA In-State Service Centers - Miami, Coral Springs, West Palm Beach	(West Palm Beach) We recommend the GTA Miami South, Miami North, Coral Springs and West Palm Beach Service Center Managers ensure that the telecommuting/virtual office forms for participation in the Alternate Work Program are completed and approved timely and participants complete the training required by the policy.
2010-0121-A2	GTA In-State Service Centers - Miami, Coral Springs, West Palm Beach-Confidential	(Miami North) Confidential
2010-0121-A2	GTA In-State Service Centers - Miami, Coral Springs, West Palm Beach-Confidential	(West Palm Beach) Confidential
2010-0121-A2	GTA In-State Service Centers - Miami, Coral Springs, West Palm Beach-Confidential	(Miami North) Confidential
2010-0121-A2	GTA In-State Service Centers - Miami, Coral Springs, West Palm Beach-Confidential	(Miami South) Confidential

IAS Engagements Outstanding Corrective Actions as of 6/30/13		
Project No.	Audit Name	Recommendation
2010-0121-A2	GTA In-State Service Centers - Miami, Coral Springs, West Palm Beach-Confidential	(West Palm Beach) Confidential
2010-0122-A	Agency Wide Environmental Ethics Audit	We recommend the SLB develop or direct the appropriate Strategic Area Committee to develop an ethics communication strategy including activities to promote ethics and values and ethics-related training at least annually.
2010-0122-A	Agency Wide Environmental Ethics Audit	We recommend the SLB consider requiring regular review and update of all ethics-related policies and procedures and an annual acknowledgement by employees.
2010-0122-A	Agency Wide Environmental Ethics Audit	We recommend the Office of Workforce Management, in consultation with the Ethics Officer and the SLB, prepare specific segments to be included in the Employee Orientation and Basic Supervisory Training on ethics, particularly regarding ethics in the hiring process, employee relationships, and vendor/client relationships.
2010-0122-A	Agency Wide Environmental Ethics Audit	We recommend executive and program management reemphasize Revenue's commitment to an ethical environment and their support for employees who report unethical or illegal behavior by reassuring employees that retaliation for reporting will not be tolerated.
2010-0122-A	Agency Wide Environmental Ethics Audit	We recommend the SLB clearly define the Ethics Program and assign authority and responsibility. We also recommend the position description(s) be updated to reflect the assignment of this responsibility.

IAS Engagements Outstanding Corrective Actions as of 6/30/13		
Project No.	Audit Name	Recommendation
2010-0122-A	Agency Wide Environmental Ethics Audit	We recommend the SLB develop or direct the appropriate Strategic Area Committee to develop goals, objectives, and strategies, and a method for monitoring compliance and evaluating the effectiveness of the ethical environment, including specific performance measures to determine whether Revenue's ethical environment meets the goals and objectives of the agency.
2011-0105-A	ISP Service Delivery Continuity Process	Confidential
2011-0105-A	ISP Service Delivery Continuity Process	Confidential
2011-0105-A	ISP Service Delivery Continuity Process	Confidential
2011-0105-A	ISP Service Delivery Continuity Process	Confidential
2011-0106-A1	CSE Payment Processing - Fund Distribution	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	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	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	Confidential
2011-0130-A	ISP Network Infrastructure Deployment Process	Confidential
2011-0130-A	ISP Network Infrastructure Deployment Process	Confidential
2011-0130-A	ISP Network Infrastructure Deployment Process	Confidential
2011-0130-A	ISP Network Infrastructure Deployment Process	Confidential

IAS Engagements Outstanding Corrective Actions as of 6/30/13		
Project No.	Audit Name	Recommendation
2011-0130-A	ISP Network Infrastructure Deployment Process	Confidential
2011-0130-A	ISP Network Infrastructure Deployment Process	Confidential
2011-0134-A2	CSE and GTA Port Richey Service Centers - Confidential	Confidential
2011-0135-A2	CSE and GTA Port Richey Service Centers - Confidential	Confidential

Appendix B

Summary of Closed Internal Investigations for FY 2012/13

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

Project	Type	Disposition
11242	Unauthorized Use of State Property, Personnel, and Equipment	Reminder Memo
11254	Misconduct off the Job	Dismissal
11259	Employment Discrimination and Retaliation	Counseling
11264	Violation of Law, Rule or Policy	Reminder Memo
11267	Confidentiality	Dismissal
11295	Unauthorized Use of State Property, Personnel, and Equipment	Referral
11296	Discourteous Behavior	Referral
11339	Theft	Referral
11344	Violation of Law, Rule or Policy	Referral
11354	Theft	No Action Required
11358	Gifts and Gratuities from Outside Sources	No Action Required
11359	Unauthorized Use of State Property, Personnel, and Equipment	Resignation
11361	Discourteous Behavior	Referral
11363	Confidentiality	Referral
11368	Misconduct off the Job	No Action Required
11371	Violation of Law, Rule or Policy	No Action Required
11372	Violation of Law, Rule or Policy	Decision Memo
11373	Violation of Law, Rule or Policy	No Action Required
11376	Unauthorized Use of State Property, Personnel, and Equipment	Resignation
11377	Violation of Law, Rule or Policy	No Action Required
11378	Violation of Law, Rule or Policy	No Action Required
11379	Confidentiality	No Action Required
11381	Dishonesty	Reminder Memo
11386	Falsification of Records	No Action Required
11387	Other	No Action Required
11388	Confidentiality	No Action Required
11389	Confidentiality	Referral
12003	Confidentiality	Referral
12004	Unauthorized Use of State Property, Personnel, and Equipment	Referral

Project	Type	Disposition
12005	Discourteous Behavior	Referral
12006	Violation of Law, Rule or Policy	No Action Required
12007	Confidentiality	No Action Required
12014	Employment Discrimination and Retaliation	Resignation
12020	Violation of Law, Rule or Policy	No Action Required
12025	Unauthorized Use of State Property, Personnel, and Equipment	No Action Required
12026	Confidentiality	No Action Required
12029	Conflict of Interest	No Action Required
12031	Theft	No Action Required
12032	Unauthorized Use of State Property, Personnel, and Equipment	No Action Required
12034	Unauthorized Use of State Property, Personnel, and Equipment	Referral
12036	Unauthorized Use of State Property, Personnel, and Equipment	No Action Required
12037	Unauthorized Use of State Property, Personnel, and Equipment	No Action Required
12038	Unauthorized Use of State Property, Personnel, and Equipment	No Action Required
12039	Unauthorized Use of State Property, Personnel, and Equipment	Decision Memo
12048	Falsification of Records	No Action Required
12052	Unauthorized Use of State Property, Personnel, and Equipment	No Action Required
12053	Confidentiality	No Action Required
12055	Personal Relationships and Department of Revenue Duties	Pending Corrective Action
12056	Falsification of Records	Resignation
12059	Confidentiality	Referral
12062	Confidentiality	Dismissal
12063	Unauthorized Use of State Property, Personnel, and Equipment	Dismissal
12066	Unauthorized Use of State Property, Personnel, and Equipment	Referral
12067	Conflict of Interest	No Action Required
12075	Confidentiality	No Action Required
12084	Theft	Resignation
12086	Violation of Law, Rule or Policy	Coaching Memo
12094	Unauthorized Use of State Property, Personnel, and Equipment	Dismissal

Project	Type	Disposition
12096	Unauthorized Use of State Property, Personnel, and Equipment	Resignation
12102	Confidentiality	No Action Required
12104	Confidentiality	No Action Required
12109	Violation of Law, Rule or Policy	No Action Required
12113	Theft	Referral
12115	Confidentiality	Referral
12116	Falsification of Records	No Action Required
12120	Violation of Law, Rule or Policy	No Action Required
12121	Confidentiality	No Action Required
12122	Conflict of Interest	No Action Required
12125	Falsification of Records	No Action Required
12129	Violation of Law, Rule or Policy	No Action Required
12130	Violation of Law, Rule or Policy	No Action Required
12133	Unauthorized Use of State Property, Personnel, and Equipment	Referral
12134	Unauthorized Use of State Property, Personnel, and Equipment	Dismissal
12144	Other	Referral
12163	Violation of Law, Rule or Policy	No Action Required
12165	Violation of Law, Rule or Policy	No Action Required
12166	Confidentiality	No Action Required
12170	Violation of Law, Rule or Policy	No Action Required
12171	Personal Relationships and Department of Revenue Duties	Reminder Memo
12172	Confidentiality	Counseling
12173	Unauthorized Use of State Property, Personnel, and Equipment	No Discipline
12175	Confidentiality	No Action Required
12176	Confidentiality	No Action Required
12178	Confidentiality	Reminder Memo
12191	Falsification of Records	No Action Required
12192	Confidentiality	No Action Required
12200	Discourteous Behavior	No Action Required
12204	Personal Relationships and Department of Revenue Duties	Pending Corrective Action
12209	Dishonesty	No Action Required
12210	Violation of Law, Rule or Policy	Referral
12214	Unauthorized Use of State Property, Personnel, and Equipment	Referral
12219	Confidentiality	No Action Required

Project	Type	Disposition
12221	Violation of Law, Rule or Policy	No Action Required
12235	Violation of Law, Rule or Policy	Referral
12243	Violation of Law, Rule or Policy	Referral
12245	Unauthorized Use of State Property, Personnel, and Equipment	No Action Required
12246	Threatening Behavior	No Action Required
12247	Unauthorized Use of State Property, Personnel, and Equipment	No Action Required
12252	Dishonesty	No Action Required
12255	Employment Discrimination and Retaliation	No Action Required
12261	Confidentiality	No Action Required
12270	Unauthorized Use of State Property, Personnel, and Equipment	Referral
12276	Violation of Law, Rule or Policy	No Action Required
12278	Violation of Law, Rule or Policy	No Action Required
12280	Confidentiality	No Action Required
12283	Unauthorized Use of State Property, Personnel, and Equipment	No Action Required
12286	Theft	No Action Required
12298	Unauthorized Use of State Property, Personnel, and Equipment	No Action Required
12300	Confidentiality	No Action Required
12301	Conflict of Interest	No Action Required
12302	Confidentiality	No Action Required
12305	Falsification of Records	No Action Required