FLORIDA DEPARTMENT OF REVENUE

Office of Inspector General

Annual Report FY 2008-2009

Internal Audit

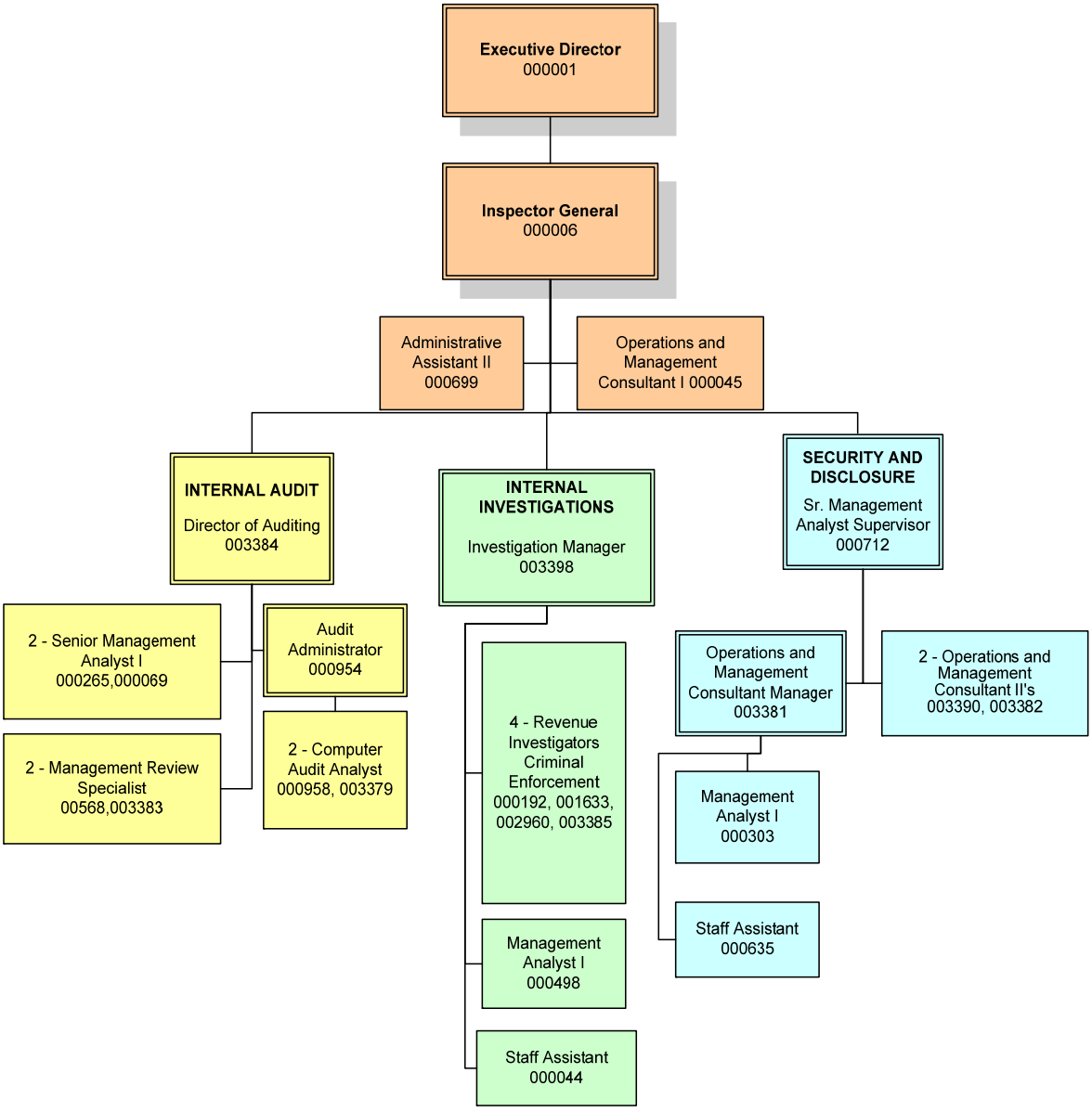
Internal Investigations

Security and Disclosure

Safety and Loss Prevention

Table of Contents

Department of Revenue
Office of Inspector General
Organizational Structure



Background

The Office of Inspector General (OIG) is established in each state agency to provide a central point of coordination 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.

OIG Responsibilities

In the Department of Revenue (Revenue), the OIG is responsible for internal audits, internal investigations, security and disclosure processes, and the Safety and Loss Prevention Program. These responsibilities are carried out by 24 full-time equivalent positions. The OIG is located in the Executive Support Program (EXEC) and the Inspector General reports directly to the Executive Director. This report is provided as required by s. 20.055, F.S. OIG's seasoned and exemplary staff strives to provide the Executive Director and department leadership with timely, 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 s. 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 him/her informed of progress made in corrective action.
- Reviewing actions taken by Revenue to improve program performance and 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 to promote economy and efficiency in the administration of Revenue's programs and operations.
- Ensuring effective coordination and cooperation between the Auditor General (AG), 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 ss. 20.055(2)(d) and 20.055(5), F.S.

Additional laws relating to the OIG include:

- Section 11.51(6), 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(2)(a)(5), 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 s. 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 s. 20.055(6), F.S., include:

- Receiving complaints and coordinating all activities of Revenue as required by ss. 112.3187–112.31895, F.S., of the Whistle-blower's Act.
- 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 Department of Law Enforcement or other law enforcement agencies, as appropriate, any information with 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, as required by s. 112.3189, F.S.

In addition to the statutory responsibilities assigned by s. 20.055, F.S., the OIG is also responsible for security and disclosure activities and the Safety and Loss Prevention Program within Revenue. The security and disclosure responsibilities include:

- Coordinating physical security of employees, facilities, information, and equipment.
- Coordinating federal and state information-sharing programs and other confidentiality and disclosure-related issues.
- Coordinating emergency management preparedness and responses.
- Maintaining and coordinating continuity of operations plans.
- Coordinating criminal history record checks.
- Conducting follow-up reviews to positive criminal history responses.
- Coordinating Revenue's Workplace Violence Program.
- Carrying out other activities to promote economy and efficiency.

Revenue's Safety and Loss Prevention Program is a comprehensive approach designed to provide a safe and healthy work environment. Safety and loss prevention responsibilities include:

- Coordinating the development and implementation of a policy and procedures for Revenue.
- Coordinating regular and periodic completion of facility and equipment safety inspections of department-operated facilities.
- Compiling Revenue's annual report on loss prevention to the Office of the Governor.
- Compiling the Division of Risk Management's annual safety evaluation report.
- Coordinating training for all employees.
- Developing, applying, and monitoring the Safety and Loss Prevention Program.
- Maintaining copies of records and reports regarding all work-related safety and loss prevention issues for Revenue.
- Providing technical assistance.
- Serving as Revenue's representative on the Interagency Advisory Council on Loss Prevention and as the Chairperson of Revenue's Safety Advisory Board.

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 Equal Employment Opportunity Commission Investigator – EEOCI	2
Certified Equal Employment Opportunity Commission Counselor - EEOCC	1
Certified Florida Crime Prevention Practitioner – CFCPP	3
Florida Crime Prevention Through Environmental Design Practitioner	4
Certified Fraud Examiner – CFE	1
Certified Information Systems Auditor – CISA	3
Certified Wireless Security Professional – CWSP	1
Certified Information Systems Security Professional – CISSP	2
Certified Internal Auditor – CIA	3
Certified Inspector General – CIG	2
Certified Inspector General Investigator – CIGI	1
Certified Public Accountant – CPA	1
Certified Public Manager - CPM	1
Certified Safety Auditor	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
- Association of Certified Fraud Examiners
- Information Systems Audit and Control Association
- InfraGard

The OIG Corner

During FY 2008/09, the OIG continued publishing articles in the DOR newsletter, the *Revenue Venue, and* Revenue's online news source, *Revenue Net News (RNN)*. 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 nonintimidating manner. In addition, articles keep employees informed of important information concerning audits, investigations, hurricane preparation, safety, discrimination, and office closures during emergency events, among other subjects. The articles were published as follows:

Office of Inspector General: The Investigation Process	September 2008
Safety: It's All About Attitude and Commitment	December 2008
Employment Discrimination: What Is It and What Do You Do?	March 2009
Hurricane Season is Here—Be Prepared!	June 2009

Annual Report Requirement

The statute 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 was not 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 the OIG's activities as required by Florida law.

Internal Audit Section

The OIG Internal Audit Section (IAS) performs audits, reviews, 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* published by the Association of Inspectors General.

According to the *Standards*, internal auditors conduct "assurance" engagements that are objective assessments of operations to provide independent opinions or conclusions regarding a process (these are generally audits and reviews). Internal auditors also conduct "consulting" engagements that are advisory in nature and generally performed at the request of a client.

The *Standards* state that "internal auditors should review operations and programs to ascertain the extent to which results are consistent with established goals and objectives to determine whether or not operations and programs are being implemented or performed as intended." At Revenue, the primary functions of the IAS are to conduct independent and objective audits and reviews of operations throughout Revenue (assurance engagements) and to provide consulting services for the purpose of improving program operations or processes (consulting engagements).

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

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

Assurance engagements result in written reports of findings and recommendations, and include responses from management. These reports are distributed internally to the Executive Director and Revenue management, and externally to the OAG.

The IAS staff provides a variety of expertise through consulting engagements. Many of the consulting engagements at Revenue involve participation in 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 the IAS and management prior to the engagement.

The IAS staff is committed to identifying and communicating innovative means to improve the way Revenue does business.

IAS Staff Certifications and Training

The IAS is comprised of three Computer Audit Analysts, two Management Review Specialists, one Senior Management Analyst I, one Audit Administrator, and the Director of Auditing. At the close of the fiscal year, there were no staff vacancies. Professional designations held by staff within the IAS include Certified Information Systems Security Professional, Certified

Information Systems Auditor, Certified Wireless Security Professional, Certified Public Accountant, Certified Public Manager, 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 Audit Directors' Roundtable meetings, Association of Inspectors General Chapter meetings, Institute of Internal Auditors meetings, IT training, and department employee training. Some of the training courses or conferences attended during FY 2008/09 included:

- Contract Auditing
- The Anatomy of Procurement Fraud
- Legal Elements of Fraud
- The Whistle-blower Act
- Importance of Soft Internal Controls in Improving Operations
- Implementing Risk-based Auditing for the Government Auditing Professional
- From Prevention to Investigation: How Technology Changed the Face of Fraud
- 7 Questions to Consider on Risk Management Practices
- Using Internal Controls to Better Manage and Monitor Programs
- Procurement Fraud
- Open Government and Confidential Information
- Key Internal Audit Considerations in this Economic Environment
- Auditing the Not-for-profit
- Enterprise Risk Management: The Art of Avoiding Surprises
- Operational Auditing: The Fundamentals
- Florida Government Technology Conference
- Standards of Conduct
- Overview of the Federal Offices of Inspectors General and Inside the OIG Investigation of Michael Vick

In addition, one staff member from the IAS completed specialized training in network administration. The staff member attended the Advanced Information Security for Technical Staff training program offered by Carnegie Mellon University's Software Engineering Institute. This workshop was designed to increase the depth of knowledge and skills of technical staff charged with administering and securing information systems and networks, and was developed around a scenario in which a production network had failed an information security audit. Participants implemented numerous technical security solutions to bring the network into compliance, working in teams to integrate these solutions throughout the enterprise. Each student had the use of a dual-boot laptop for the duration of the workshop, as well as direct, administrative access to a wide variety of networked systems.

Annual Risk Assessment and Audit Plan

Each year the IAS assesses the operations of Revenue to identify areas with the highest levels of risk (probability of an adverse action). Criteria used for the risk assessment include the complexity of operations, geographic dispersion, management interest, external oversight, controls, dollar volume/materiality, asset liquidity, changes in procedures and personnel, results of prior audits, public exposure, and other criteria as appropriate. Input from executive

management, program directors, process owners, and subprocess owners were considered in this year's risk assessment.

Using the results of the risk assessment, the IAS develops an annual audit plan. The audit plan includes the areas to be audited or reviewed, timing of the audits/reviews, budgeted hours, and assignment of staff. The audit plan is approved by 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. The OIG provides status reports on internal audit findings and recommendations to department management annually.

The IAS improved its corrective action plan follow-up process by creating a standard template that programs could use to summarize their open corrective action plans for presentation at regularly scheduled executive briefings. The roles and responsibilities for internal audit staff were refined to include working with the programs to ensure all open corrective action plans are accurately reflected in the executive briefing document, attending all program executive briefings, and being prepared to participate in any discussion about the corrective action plans.

As required by s. 20.055(5)(h), F.S., the OIG monitors the accomplishment of Revenue's responses to reports issued by the AG and OPPAGA. The OIG is also required to provide a written response to the Executive Director on the status of corrective actions taken no later than six months after a report is published. A copy of the response is also provided to the Joint Legislative Auditing Committee (JLAC). Additionally, as required by s. 11.51(6), F.S., OPPAGA submits requests no later than 18 months after the release of a report to Revenue to provide data and other information describing specifically what Revenue has done to respond to recommendations contained in its reports. The OIG is responsible for coordinating these status reports and ensuring that they are submitted within the established time frames.

Performance Measures

In accordance with s. 20.055(2)(a), F.S., the OIG serves in an advisory capacity to program management and staff during the development of performance measures, standards, and procedures.

Assurance Engagements Conducted During FY 2008/09

During FY 2008/09, the IAS completed 13 assurance engagements. Below is a summary of activity for the year:

Security Administration

The purpose of this audit was to review the administrative controls utilized by the IT Security Process within the Information Services Program (ISP).
The objectives of this engagement were to:

- Ensure that risk identification and assessment are adequately conducted by the auditee;

- Determine if adequate security policies and procedures are in place before the deployment of new IT resources;
- Ensure that existing IT security policies and procedures are adequately maintained and updated;
- Determine if IT security activities are adequately enforced throughout the agency; and
- Ensure that IT contractors are following applicable IT security policies and procedures.

Six recommendations were made in the areas of risk assessment, security policy management, information resource administration, and contractor background checks.
Specific details of the findings and recommendations are provided to the Executive Director but not disclosed in this report due to the confidential subject matter.

GTA Key West Service Center
The purpose of this audit was to determine if the collections process in the service center is in compliance with *Florida Statutes, Florida Administrative Code,* and Revenue polices and procedures. The objectives of this engagement were to:

- Determine if Revenue established policies and procedures for the handling of worthless checks, filing of tax warrants, referral of cases for criminal investigation and the Tax Collection Enforcement (TCE) Diversion Program, and write-off of receivables are sufficient;
- Determine whether the service center is processing worthless checks in accordance with *Florida Statutes, Florida Administrative Code,* and Revenue established policies and procedures;
- Determine whether the service center is processing delinquent cases in accordance with Revenue established policies and procedures for filing of tax warrants;
- Determine whether the service center is referring cases for external criminal investigations in accordance with Revenue established policies and procedures and the State Attorney Interagency Memorandum Of Understanding (MOU) and Bad-Check Diversion Program;
- Determine whether the service center is referring cases for internal investigations in accordance with Revenue established policies and procedures for the TCE Diversion Program; and
- Determine whether write-offs of receivables by the service center were conducted in accordance with Revenue established policies and procedures.

The audit concluded collection activities were in general compliance with applicable policies, procedures, laws, and regulations. However, policies and procedures needed improvement. The audit recommended:

1. Program Management update the Revenue Specialist Handbook to provide comprehensive guidance to service center employees, including references to SUNTAX requirements and guidance provided through GTA Procedure Bulletins and e-mails;
2. Program Management develop and implement a timeline and structure to provide service center employees guidance on the specific enforcement actions required at each dunning level. In order to escalate collection efforts to the next dunning level, required enforcement actions should be clearly stated; and
3. Program Management take steps to improve communication between the collections and investigations personnel by encouraging open and direct discussions between all personnel who may go outside the current chain of command.

Follow-Up Audit on the AG Federal Awards Audit for FY 2007/08
The purpose of this audit was to report on the status and adequacy of the programs' corrective action plans (CAPs) to address the findings and audit recommendations contained in AG Report No. 2008-141. The AG's report contained three audit findings and recommendations involving the Florida Department of Revenue (FDOR). The follow-up audit of these three findings concluded:

1. AG Finding No. FA07-011 has been adequately addressed by the Administrative Services Program (ASP), and the corrective action plan has been fully implemented;
2. AG Finding No. FA07-013 has been adequately addressed by GTA, and the corrective action plan has been fully implemented; and
3. AG Finding No. FA07-048 is in the process of being addressed, and the corrective action plan is still open.

GTA Rewards
The purpose of this audit was to evaluate the adequacy and effectiveness of the controls associated with the GTA Rewards Program process. The objectives of this engagement were to:

- Determine whether the Rewards Program is in compliance with statutes, rules, policies and procedures;
- Determine if internal controls associated with the Rewards Program are adequate; and
- Determine the efficiency of the Rewards Program process.

The audit did not reveal any noncompliance with Florida Statutes or rules. However, some internal controls were found to be inadequate and ineffective, and there were some inefficiencies within the Rewards Program. Several issues were noted where improvements were needed and the audit recommended:

1. GTA Program management develop, approve, and maintain comprehensive and detailed written procedures for the Rewards Program process;
2. A quality review process be established to ensure the *Case Closeout Checklist* contains sufficient, detailed information to substantiate the percentage of rewarded compensation outlined within Rule 12-18.003, F.A.C.;
3. Rewards Program staff enforce the existing requirement to perform a reconciliation of the status of all pending claims once per calendar quarter; and
4. Management establish Rewards Program performance metrics and monitor those metrics for comparison and analysis of variances between actual performance and expected performance so corrective action can be taken as necessary to improve effectiveness and efficiency of the process.

Follow-Up Audit on the AG Audit of SUNTAX/IMS IT Audit
The objective of this engagement was to verify the adequacy and accuracy of corrective action plans submitted by ISP and GTA in response to the AG's audit of SUNTAX and IMS, AG Report No. 2008-0097. The scope of work was limited to the responses provided by ISP and GTA within the CAP documents. The corrective action plans were reviewed for accuracy, completeness and adequacy. Details of some of the findings and recommendations are confidential. Nonetheless, the follow-up audit concluded that:

1. AG Finding No. 1 is being addressed by the action steps and the corrective action plan is in the process of being implemented;
2. AG Finding No. 2 is being addressed, and the corrective action plan is in the process of being implemented;
3. AG Finding No. 3 has been partially addressed, and the corrective action plan has been partially implemented;
4. With one exception, AG Finding No. 4 is being addressed by the action steps; and
5. AG Finding No. 5 is being adequately addressed, and the corrective action plan is in the process of being implemented.

One additional recommendation was made in this audit, the specific details of which are confidential.

Child Support Enforcement (CSE) Debit Cards
The objectives of this engagement were to determine whether:

- The Debit Card Program is in compliance with applicable laws, rules, regulations, industry standards, and contract terms;
- The Debit Card Program is working as intended; and
- Controls are adequate to ensure that debit card distributions are appropriately authorized and disbursed, and accurately reported.

The audit determined that the Debit Card Program is generally in compliance with applicable laws, rules, regulations, industry standards, and relevant contract terms. Also, the Debit Card Program is generally working as intended—it has reduced the number of instances of lost or stolen payments, reduced the waiting time for payments, and reduced the potential costs of check cashing fees for those custodial parents who utilize debit cards instead of checks. Although the audit did not specifically identify any unauthorized, inaccurate, or untimely transactions, several issues were noted where improvements were needed. The audit recommended:

1. The CSE Program follow established procedures and complete the verification of IV-D accounts;
2. The CSE Program consider adding an additional step to the on-site monitoring program which would require periodic tracing of a sample of disbursements authorized by Revenue to the individual Electronic Payment Processing Information Control (EPPIC) accounts; and
3. That an audit performed in accordance with Statement on Auditing Standards No. 70 (SAS 70), or other operational audit of the State Disbursement Unit (SDU) by an independent CPA firm, be performed annually to help ensure controls over collections, disbursement, and reporting are adequate. Such audits would provide additional assurance that funds are accounted for and reported correctly.

Follow-Up Audit on Property Tax Oversight (PTO) Corrective Action Plans
The objective of this audit was to review the corrective action plans developed by PTO and to provide assurance that the corrective action plans adequately address the deficiencies noted in prior audits. The prior audit reports included in this review were those issued by Revenue's

OIG, as well as those issued by external entities such as the AG and OPPAGA, for which corrective action plans were not yet completed.

The audit found that program management has recently addressed noted deficiencies and fully implemented the corrective action plans for two prior audit findings and corrective actions have not been fully implemented for nine prior audit findings.

No additional recommendations resulted from this audit.

Follow-Up Audit of ASP Corrective Action Plans
The objective of this audit was to review the corrective action plans developed by ASP to provide assurance that the corrective action plans adequately address the deficiencies noted in prior audits. The prior audit reports included in this review were those issued by Revenue's OIG, as well as those issued by external entities such as the AG and OPPAGA, for which corrective action plans were not yet completed.

The audit found that program management has recently addressed noted deficiencies and fully implemented the corrective action plans for one prior audit finding and corrective actions have not been fully implemented for three prior audit findings.

One recommendation was made for ASP to work with ISP management to ensure a solution is developed to establish accurate transaction logging.

Follow-Up Audit of CSE Corrective Action Plans
The objective of this audit was to review the corrective action plans developed by CSE to provide assurance that the corrective action plans adequately address the deficiencies noted in prior audits. The prior audit reports included in this review were those issued by Revenue's OIG, as well as those issued by external entities such as the AG and OPPAGA, for which corrective action plans were not yet completed.

The audit found that program management has recently addressed noted deficiencies and fully implemented the corrective action plans for two prior audit findings and corrective actions have not been fully implemented for eight prior audit findings.

No additional recommendations resulted from this audit.

Follow-Up Audit of General Tax Administration (GTA) Corrective Action Plans
The objective of this audit was to review the corrective action plans developed by GTA to provide assurance that the corrective action plans adequately address the deficiencies noted in prior audits. The prior audit reports included in this review were those issued by Revenue's OIG, as well as those issued by external entities such as the AG and OPPAGA, for which corrective action plans were not yet completed.

The audit found that program management has recently addressed noted deficiencies and fully implemented the corrective action plans for two prior audit findings and corrective actions have not been fully implemented for nine prior audit findings.

No additional recommendations resulted from this audit.

Internet Tax Applications
The objectives of this engagement were to:

- Determine if adequate procedures for the secure and controlled development of Internet tax applications are in place;
- Determine if policies and procedures are in place to address security breaches to Internet tax applications and Internet web servers; and
- Determine if applications are being maintained and monitored, and backups are being performed in accordance with appropriate policies and procedures.

The audit determined that departmental policies and procedures are in place for the secure and controlled development, maintenance, and monitoring of applications within Revenue. However, established policies and procedures were not consistently followed during application development and maintenance, and improvement can be made in addressing the possibility of an interruption of tax services to web applications.

The audit recommended:

1. All Revenue tax applications utilize the mandatory tasks of the adopted ISDM and that management monitor usage;
2. ISP compare Revenue's web standards to the *Florida Administrative Code* and NIST to ensure that Revenue's web standards are sufficient to secure Internet applications;
3. ISP update DOR-WEB-001 and DOR-SEC-001 to include detailed guidance for the security of Internet applications and to ensure compliance with industry standards;
4. ISP include in DOR-WEB-001 and DOR-SEC-001 requirements for an independent Quality Assurance Review (QAR) to be performed by Revenue's Service Support Release Management program as application code is being developed, or when significant changes in an Internet application are performed to ensure that security standards are effective;
5. ISP web page development and maintenance procedures include the requirement that the "Security Statement" is consistently titled and in the same location on all web pages so that users can easily identify it;
6. ISP review all web pages and ensure that "Security Statement" standards, such as those requiring the VeriSign logo, are being followed, and all pages are corrected that are not currently in compliance. This should be a standard step in the QAR process;
7. The Confidential Information Officer of the Office of Executive Director review regulations and industry best practices that may improve Revenue's privacy and security statements, and coordinate with ISP to facilitate the implementation of procedural requirements;
8. GTA contract management personnel take the necessary steps to ensure all contractual provisions which benefit Revenue are fulfilled;
9. GTA in consultation with ISP review Baca, Stein, White, and Associates' (BSWA) emergency preparedness plan to determine if it is adequate to handle interruption of services. If the plan is determined not to be adequate, we recommend GTA request BSWA to submit an emergency preparedness plan that meets industry guidelines of NIST Pub 800-34, Rule 60DD, and Revenue procedures;
10. ISP evaluate third-party vendors' security practices when negotiating or reviewing IT contracts;

11. ISP in consultation with Security and Disclosure develop standard contract language for an emergency preparedness plan that meets the minimum procedures and specifications of industry guidelines of NIST Pub 800-34, Rule 60DD, and Revenue procedures; and
12. GTA require criminal background checks be performed on all BSWA employees who have access to Revenue information resources and that those checks meet contract requirements.

PTO Central Assessment Process
The objectives of this engagement were to determine if controls are adequate to ensure:

- Compliance with applicable laws and regulations; and
- The efficiency and effectiveness of the Central Assessment process.

The audit determined that existing controls are adequate to ensure compliance with applicable laws and regulations, and to ensure the efficiency and effectiveness of the Central Assessment process. We found that the data utilized in analyses were adequately supported, calculations used in those analyses were correct, and notice of values were provided to the railroads timely. Our review of processes and work flows did not identify any significant inefficiencies. The appraisal files we reviewed demonstrated that appraisals and value apportionments were done in compliance with state law and Revenue procedures with one exception. Value reconciliations were not always documented in the appraisal reports as required.

The audit recommended the Program ensure that value reconciliations are documented in each appraisal report as required by *Uniform Standards of Professional Appraisal Practice* and PTO's written procedures.

System Hosting – Linux Administration The purpose of this audit was to review the security of the Linux servers, which affects the security of the applications hosted on the servers. The scope of this audit included Linux servers in use on the Revenue network between July 2008 and April 2009.

The objectives of this engagement were to:

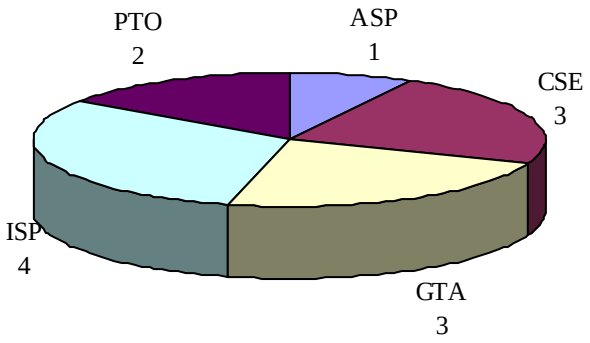
- Determine whether Linux servers are being adequately patched;
- Determine whether only necessary services are running on Linux servers;
- Determine whether Linux servers are being securely configured;
- Determine whether user access is being adequately controlled on Linux servers; and
- Determine whether audit trails are adequately maintained and monitored on Linux servers.

The audit found there are adequate departmental policies and procedures in place for the physical security of the Linux servers and applications on the servers. However, policies and procedures had not been established for some security functions. Also, ISP and GTA had not consistently followed existing policies and procedures during server configuration and maintenance.

Recommendations were made in the areas of server maintenance, user access, policy development, existing policy enforcement and training. Specific details of the findings and recommendations are provided to the Executive Director but not disclosed in this report due to the confidential subject matter.

The following chart shows the number of assurance engagements conducted by program.

Internal Audits for FY 08/09



Consulting Engagements Conducted During FY 2008/09

During FY 2008/09, the IAS completed 26 consulting engagements, 3 of which resulted in the issuance of management letters or a final report. The IAS has taken a more proactive, customer-driven approach in Revenue's risk management and governance activities by providing management consulting and advisory services for the purpose of improving program operations or processes. The IAS staff participated on teams with CSE, ISP, EXE, and GTA to recommend internal controls that help achieve program goals and objectives. The IAS staff also participated on teams that addressed agency-wide topics such as computer security and the anticipated move to the Southwood complex.

Additionally, IAS staff provided detailed reviews of five draft policies prior to presentation to the Strategic Leadership Board (SLB). These reviews provide the Board with information concerning risk, compliance, internal controls, and other pertinent information to assist in making an informed decision concerning policy. IAS staff also provided a detailed review of the proposed ASP Contract Manager Training course.

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

Executive Director's Autopen Signatures
The purpose of this project was to review the use of the Autopen in lieu of the Executive Director's personal signature. The objectives of this review were to:

1. Evaluate the adequacy of written policies and procedures;
2. Evaluate the adequacy of internal controls;
3. Determine compliance with policies and procedures; and
4. Determine whether there are more efficient or effective methods.

This consultant project provided reasonable assurance to the Executive Director and Chief of Staff that Autopen and electronic signatures are adequately controlled, and usage is in accordance with the authority granted by the Executive Director. Despite the lack of written policies and procedures, it appeared that the Executive Director's staff, Recognition Office staff, and Communication and Professional Development (CPD) staff are complying with the expectations of the Executive Director in the use of her Autopen or electronic signature.

We recommended the development of written policies and procedures for use of the Executive Director's Autopen and electronic signatures that include:

1. Requirements to maintain written approvals of those employees authorized to use the Executive Director's electronic or Autopen signature;
2. Requirements to develop and maintain an inventory of types of documents that are authorized for Autopen or electronic signature;
3. Requirements that a log be used, which outlines the type and number of documents signed using the Autopen or electronic signature, as well as information regarding the program, process, office, and person who used the Autopen and electronic signature;
4. Requirements for additional segregation of duties such as the signature plate being maintained in a different location and controlled by a different employee than the employee who has a key to the machine;
5. Requirements for routine, independent, managerial monitoring of Autopen and electronic signature use, including a review of logs of documents signed, and written approvals authorizing usage; and
6. Instructions for destroying obsolete signature plates.

We also recommended that the former Executive Director's signature plate be destroyed immediately, with adequate oversight and documentation.

Six-Month Follow-Up on AG Report No. 2009-024,
GTA Taxpayer Refunds and Prior Audit Findings
The purpose of this project was to provide the Executive Director a six-month written update on the status of the agency's corrective action plans to address the five findings contained in AG Report No. 2009-024, *Department of Revenue Taxpayer Refunds and Prior Audit Follow-Up.*

The status update revealed that two of the five corrective action plans were complete, two were partially complete, and one remained open. Specific details of the findings and recommendations are provided to the Executive Director but not disclosed in this report due to the confidential subject matter.

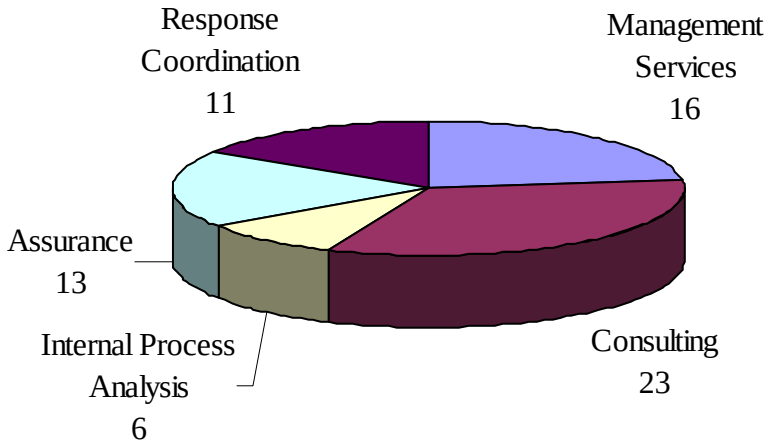
2008 Florida Risk Assessment Survey
Florida Statutes require each agency to "conduct, and update every 3 years, a comprehensive risk analysis to determine the security threats to the data, information, and IT resources of the agency," and to "ensure that periodic internal audits and evaluations of the agency's security program for the data, information, and IT resources of the agency are conducted." The Agency for Enterprise Information Technology (AEIT) developed a process to help state agencies satisfy this statutory requirement through the 2008 State of Florida Risk Assessment. Our office evaluated Revenue's responses to the risk assessment survey questions, reviewed supporting documentation provided by management and IT staff, attested to the reasonableness of the responses, and delivered the completed Risk Assessment to the AEIT prior to its due date**.**

Other IAS Services
These services include Internal Process Analysis, Management Services, and Response Coordination.

For example, the IAS staff act as agency coordinators for the Florida Single Audit Act (FSAA). This includes acting as a liaison with program FSAA leads, helping identify legislative effects on Revenue related to the FSAA, handling inquiries from the public or other state agencies, as well as assisting in the development of Revenue FSAA Administrative Procedures.

Additionally, IAS staff attends all monthly and quarterly program executive briefings, monitors all of the programs' corrective action plans to address prior audit findings, coordinates all external audits conducted by other entities, and coordinates Revenue's responses to those audits.

Types of Internal Audit Projects for FY 08/09



Other IAS Accomplishments During FY 2008/09
The IAS made several improvements in its processes during the past fiscal year. These include:

- Continued to refine the enterprise-wide risk assessment.

- Continued to refine use of the Audit Leverage software package to automate audit work papers.
- Refined the audit response process to ensure program responses are reviewed by executive management. When a preliminary and tentative audit report is issued by either the Office of Inspector General or an external auditor, the IAS implemented a new process to include a mandatory meeting between the OIG, the Program Director, the Executive Director, Deputy Director, and Chief of Staff to discuss the program's proposed response to each audit finding. This meeting provides executive management an opportunity to review and comment on the program's draft responses and corrective action plans before finalizing. This change to the audit response process has brought heightened awareness of significant issues and risks to Revenue. It helps ensure executive management and program management understand risks to Revenue, and that executive management is in agreement that the program's proposed corrective action plan is the best course of action to address each audit finding. Risk acceptance has been raised to the highest level of the organization.
- Improved the corrective action plan follow-up process by ensuring open corrective action plans are presented at each program's executive briefing. This process change helps facilitate discussion between executive management and program management, and helps ensure programs report on their progress toward addressing outstanding audit issues. This change has also brought heightened awareness to corrective action plans, especially those that have been open for a long period and for which there was difficulty in meeting the original projected completion dates.

The IAS participated in a Quality Assessment Review performed by the AG for the period July 2007 through June 2008. The AG concluded that the quality assurance program related to the Office of Inspector General's internal audit activity provided reasonable assurance of conformance to applicable auditing standards. The AG also concluded that the Office of Inspector General generally complied with those provisions of s. 20.055, F.S., governing the operation of state agencies' offices of inspector general and internal audit activities. No adverse findings or recommendations for improvement were reported.

The Director of Auditing volunteered on a Risk Assessment Committee established by the Chief Inspector General to help identify risks associated with the receipt and expenditure of funds related to the American Recovery and Reinvestment Act of 2009. The committee developed a Risk Readiness Review Questionnaire to assist state agency inspectors general in assessing the implementation of internal controls, which should help mitigate the risk of fraud, waste, or abuse, in programs that will be or have received federal stimulus funds.

Another noteworthy accomplishment is that one staff member obtained the Certified Information Systems Auditor (CISA) professional designation.

Outstanding Corrective Action for Prior Audit Reports

IAS Engagements Outstanding Corrective Action as of 6/30/09		
Project No.	**Audit Name**	**Recommendation**
2004-0141	CSE Contract Management Audit	2. We recommend that management include staff roles and responsibilities in the development and implementation of their policies and procedures manual.
2004-0313	GTA Underpayment Resolution Audit	1.1 We recommend management develop timelines for progression of a receivable from dunning level 6 through 17. This will give employees and managers the time expectations as to when a receivable should escalate through the dunning level process.
2004-0313	GTA Underpayment Resolution Audit	3. We recommend management notify employees that all STIP agreements must be entered into SAP and there will no longer be informal STIP agreements established.
2004-0421	Security Incident Mitigation	2. Confidential
2005-0038	System Hosting Business Process	1.2 Confidential
2005-0038	System Hosting Business Process	2. Confidential
2005-0041	Real Property Roll Compliance	1d. We recommend that the PTO Program establish a team to research the viability of requesting electronic data from property appraisers' CAMA systems before and after roll review to conduct data matching for testing property appraisers' mass appraisal change assertions.
2005-0041	Real Property Roll Compliance	3. We recommend PTO develop and put into operation an interim database, with assistance from the Office of Resource Management, while a more comprehensive data management system is developed with assistance from ISP and the Office of Resource Management.

IAS Engagements Outstanding Corrective Action as of 6/30/09		
Project No.	**Audit Name**	**Recommendation**
2005-0051	Financial Data Update Sub-Process	1.b. In addition, we recommend GTA continue to examine the feasibility of processing payments and returns within SAP at the service centers.
2005-0052	User Account Maintenance	2. Confidential
2005-0052	User Account Maintenance	3. Confidential
2005-0052	User Account Maintenance	4. Confidential
2006-0046	GTA Delinquency Process	1. We recommend GTA review SAP roles and their access rights versus employees' job duties and responsibilities and further customize roles to limit access necessary to perform assigned duties and responsibilities.
2006-0046	GTA Delinquency Process	2.1 We recommend GTA, in consultation with the Office of the General Counsel (OGC), address the issue of delinquency withdrawals either by statute, rule, and/or policies and procedures.
2006-0046	GTA Delinquency Process	3. We recommend GTA address, via rule or policies and procedures, delinquency withdrawals to include documentation requirements of supervisory oversight of these withdrawals.
2006-0046	GTA Delinquency Process	4. We continue to recommend GTA develop and implement a comprehensive set of policies and procedures for all GTA collection personnel statewide.
2006-0046	GTA Delinquency Process	5. We recommend GTA management develop and implement clear, uniform criteria via policies and procedures, with timeliness expectations of collections personnel for the clearing of delinquencies and to ensure supervisory monitoring of these expectations.
2006-0055	ASP Technology Audit	3. We recommend ASP develop specific procedures, methods, and management tools in order to effectively track IT resources.

IAS Engagements Outstanding Corrective Action as of 6/30/09		
Project No.	**Audit Name**	**Recommendation**
2006-0055	ASP Technology Audit	4. Confidential
2006-0056	ISP Telecommunications Audit	1. We recommend ISP direct resources to ensure that adequate procedures are developed and maintained.
2006-0056	ISP Telecommunications Audit	2.1 We recommend that the Telecommunications Section implement an ISDM.
2006-0056	ISP Telecommunications Audit	2.2 We recommend that the Telecommunications Section ensure that all of its computer applications are adequately documented.
2006-0056	ISP Telecommunications Audit	3. We recommend that the Telecommunications Section work with department management to develop procedures that will provide verification of telecommunications invoices.
2006-0056	ISP Telecommunications Audit	4. Confidential
2007-0049	System Hosting – Linux	1.1 Confidential
2007-0049	System Hosting – Linux	1.2 Confidential
2007-0049	System Hosting – Linux	1.3 Confidential
2007-0049	System Hosting – Linux	2.1 Confidential
2007-0049	System Hosting – Linux	2.2 Confidential
2007-0049	System Hosting – Linux	2.3 Confidential
2007-0049	System Hosting – Linux	2.4 Confidential
2007-0049	System Hosting – Linux	3.1 Confidential
2007-0049	System Hosting – Linux	3.2 Confidential
2007-0049	System Hosting – Linux	3.3 Confidential
2007-0049	System Hosting – Linux	3.4 Confidential

IAS Engagements Outstanding Corrective Action as of 6/30/09		
Project No.	**Audit Name**	**Recommendation**
2007-0049	System Hosting – Linux	3.5 Confidential
2007-0049	System Hosting – Linux	4.1 Confidential
2007-0049	System Hosting – Linux	4.2 Confidential
2007-0049	System Hosting – Linux	4.3 Confidential
2007-0049	System Hosting – Linux	5.1 Confidential
2007-0049	System Hosting – Linux	5.2 Confidential
2007-0049	System Hosting – Linux	5.3 Confidential
2007-0065	ISP Security Administration	1. Confidential
2007-0065	ISP Security Administration	2.1 Confidential
2007-0065	ISP Security Administration	2.2 Confidential
2007-0065	ISP Security Administration	3.1 Confidential
2007-0065	ISP Security Administration	4. Confidential
2007-0065	ISP Security Administration	5. Confidential
2007-0053	ISP Web Applications Audit	1.1 Confidential
2007-0053	ISP Web Applications Audit	1.2 Confidential
2007-0053	ISP Web Applications Audit	1.3 Confidential
2007-0053	ISP Web Applications Audit	1.4 Confidential
2007-0053	ISP Web Applications Audit	2. Confidential
2007-0053	ISP Web Applications Audit	3. Confidential
2007-0053	ISP Web Applications Audit	4.1 Confidential
2007-0053	ISP Web Applications Audit	4.2 Confidential
2007-0053	ISP Web Applications Audit	4.3 Confidential
2007-0053	ISP Web Applications Audit	4.4 Confidential

IAS Engagements Outstanding Corrective Action as of 6/30/09		
Project No.	**Audit Name**	**Recommendation**
2007-0053	ISP Web Applications Audit	5.1 Confidential
2007-0053	ISP Web Applications Audit	5.2 Confidential
2007-0067	Internet Tax Applications	1. We recommend that all Revenue tax applications utilize the mandatory tasks of the adopted ISDM and that management monitor usage.
2007-0067	Internet Tax Applications	2.1 We recommend ISP compare Revenue's web standards to the *Florida Administrative Code* and NIST to ensure that Revenue's web standards are sufficient to secure Internet applications.
2007-0067	Internet Tax Applications	2.2 We recommend ISP update DOR-WEB-001 and DOR-SEC-001 to include detailed guidance for the security of Internet applications and to ensure compliance with industry standards.
2007-0067	Internet Tax Applications	2.3 We recommend ISP include in DOR-WEB-001 and DOR-SEC-001 requirements for an independent QAR to be performed by the Department's Service Support Release Management program as application code is being developed or when significant changes in an Internet application are performed to ensure that security standards are effective.
2007-0067	Internet Tax Applications	3.1 We recommend that ISP web page development and maintenance procedures include the requirement that the "Security Statement" is consistently titled and in the same location on all web pages so that users can easily identify it.
2007-0067	Internet Tax Applications	3.2 We recommend that ISP review all web pages and ensure that "Security Statement" standards, such as those requiring the VeriSign logo, are being followed and all pages are corrected that are not currently in compliance.

IAS Engagements Outstanding Corrective Action as of 6/30/09		
Project No.	**Audit Name**	**Recommendation**
2007-0067	Internet Tax Applications	3.3 We recommend that the Confidential Information Officer of the Office of Executive Director review regulations and industry best practices that may improve Revenue's privacy and security statements, and coordinate with ISP to facilitate the implementation of procedural requirements.
2007-0067	Internet Tax Applications	4.1 We recommend GTA contract management personnel take the necessary steps to ensure all contractual provisions which benefit Revenue are fulfilled.
2007-0067	Internet Tax Applications	4.2 We recommend GTA in consultation with ISP review BSWA's emergency preparedness plan to determine if it is adequate to handle interruption of services. If the plan is determined not to be adequate, we recommend GTA request BSWA to submit an emergency preparedness plan that meets industry guidelines of NIST Pub 800-34, Rule 60DD, and Revenue procedures.
2007-0067	Internet Tax Applications	4.3 We recommend that ISP evaluate third-party vendors' security practices when negotiating or reviewing IT contracts.
2007-0067	Internet Tax Applications	4.4 We recommend ISP in consultation with Security and Disclosure develop standard contract language for an emergency preparedness plan that meets the minimum procedures and specifications of industry guidelines of NIST Pub 800-34, Rule 60DD, and Revenue procedures.
2007-0067	Internet Tax Applications	5.1 We recommend GTA require criminal background checks be performed on all BSWA employees who have access to Revenue information resources and that those checks meet contract requirements.

IAS Engagements Outstanding Corrective Action as of 6/30/09		
Project No.	**Audit Name**	**Recommendation**
2007-0068	CSE Debit Card Program	1.1 We recommend the CSE Program follow established procedures and complete the verification of IV-D accounts.
2007-0068	CSE Debit Card Program	1.2 We recommend the CSE Program consider adding an additional step to the on-site monitoring program which would require periodic tracing of a sample of disbursements authorized by DOR to the individual EPPIC accounts.
2007-0068	CSE Debit Card Program	2. We recommend that an audit performed in accordance with Statement on Auditing Standards No. 70 (SAS 70), or other operational audit of the SDU by an independent CPA firm, be performed annually to help ensure controls over collections, disbursement, and reporting are adequate.
2007-0072	GTA Rewards Program	1. We recommend GTA Program management develop, approve, and maintain comprehensive and detailed written procedures for the Rewards Program process.
2007-0072	GTA Rewards Program	2. To ensure compliance with *Florida Administrative Code*, we recommend a quality review process be established to ensure the *Case Closeout Checklist* contains sufficient, detailed information to substantiate the percentage of rewarded compensation outlined within Rule 12-18.003, F.A.C.
2007-0072	GTA Rewards Program	3. We recommend Rewards Program staff enforce the existing requirement to perform a reconciliation of the status of all pending claims once per calendar quarter.

IAS Engagements Outstanding Corrective Action as of 6/30/09		
Project No.	**Audit Name**	**Recommendation**
2007-0072	GTA Rewards Program	4. We recommend management establish Rewards Program performance metrics and monitor those metrics for comparison and analysis of variances between actual performance and expected performance so corrective action can be taken as necessary to improve effectiveness and efficiency of the process.
2007-0076	GTA Key West Service Center	1.1 We continue to recommend that program management update the Revenue Specialist Handbook to provide comprehensive guidance to service center employees, including references to SUNTAX requirements and guidance provided through GTA Procedure Bulletins and e-mails.
007-0076	GTA Key West Service Center	1.2 We continue to recommend that program management develop and implement a timeline and structure to provide service center employees guidance on the specific enforcement actions required at each dunning level. In order to escalate collection efforts to the next dunning level, required enforcement actions should be clearly stated.
2007-0076	GTA Key West Service Center	1.3 We recommend that program management take steps to improve communication between the collections and investigations personnel by encouraging open and direct discussions between all personnel that may go outside the current chain of command.
2008-0107	PTO Central Assessment Process	1. We recommend the Program ensure that value reconciliations are documented in each appraisal report as required by USPAP standards, and PTO's written procedures.

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 investigative staff. The preliminary review is used to filter complaints to ensure that investigative resources are used effectively and efficiently so that only complaints containing significant allegations are investigated. Established criteria are used to initially evaluate each complaint to determine the appropriate course of action. When determined via the preliminary review that a full investigation is warranted, an investigation is initiated.

Internal Investigations Section Accomplishments during FY 2008/09

- Participated on the sub-teams tasked with developing accreditation standards for Florida Inspectors General investigations units. Florida's Chief Inspector General initiated this effort.
- Established a goal of October 2010 to become accredited by the Commission for Florida Law Enforcement Accreditation (CFA).
- Two staff members and the Inspector General attended a 16-hour Accreditation Manager training course sponsored by the CFA.
- One staff member attended a 16-hour Accreditation Assessor Training sponsored by the CFA.
- Continue to update Investigative policy and procedures to be aligned with the accreditation standards.
- One staff member attended a two-day public records management training course to help in the management of public records requests received by the Investigations Section and also file retention.
- Assisted in the development of a complaint intake system. The system called "Ethics Link" was deployed to all Revenue employees in November 2008.

Summary of IIS Closed Cases

Investigation Summaries 2008/09

A number of significant investigations were conducted during FY 2008/09. The following are highlights of some of these cases:

Dishonesty/Lying
The OIG received information that an employee received assistance from another employee in securing a promotion with Revenue by reviewing interview questions for the position. The employee claimed the questions were intentionally left on the printer for him to review by an employee prior to his interview. The employee viewed the questions and returned them to the printer. The employee resigned from Revenue. The employee who assisted admitted to printing and leaving the interview questions on her office printer for the other employee. The employee was dismissed from Revenue.

Misconduct Off The Job/Theft
The OIG received information that an employee knowingly signed for the purchase of an item with the debit card of another employee. The debit card was stolen from another employee earlier that day. The employee was viewed by a store surveillance camera standing at the counter with her husband and signing the debit card of another employee. The employee claimed that she thought the debit card her husband told her to sign was her debit card. After realizing the card was not hers, the employee said she signed the debit card so that there would not be a confrontation with her husband. The employee was dismissed from Revenue.

Poor Judgment/Conflict of Interest
The OIG received information that an employee who is responsible for facilitating retirement for Revenue employees, processed her own retirement and authorized an accumulated amount of leave payout for herself, without the knowledge of her immediate supervisor. The employee did not seek guidance from the supervisor when she was processing her retirement paperwork and leave payout. The employee claimed that she was unaware that she had to notify her supervisor that she was entering retirement and believed it was acceptable for her to process her own retirement and leave payout. The investigation did not reveal that the employee received any benefit she was not entitled. Subsequently, the employee retired from Revenue.

Theft or Stealing
The OIG received information that an employee had taken a taxpayer's cash payment and used it for personal use. When a manager was reviewing aging accounts, one taxpayer's account came into question. The manager contacted the taxpayer and questioned his account. The taxpayer said he paid the taxes on his account in cash and received a receipt from the employee. The receipt the taxpayer received was not the standard receipt Revenue issues. The taxpayer said he was contacted by the employee after he made the cash payment at the office and was told that a "corrected receipt" would be mailed to him. Employee was interviewed and admitted to taking the taxpayer's payment of approximately $3,000 for personal use. The employee was dismissed from Revenue and the case was referred to law enforcement.

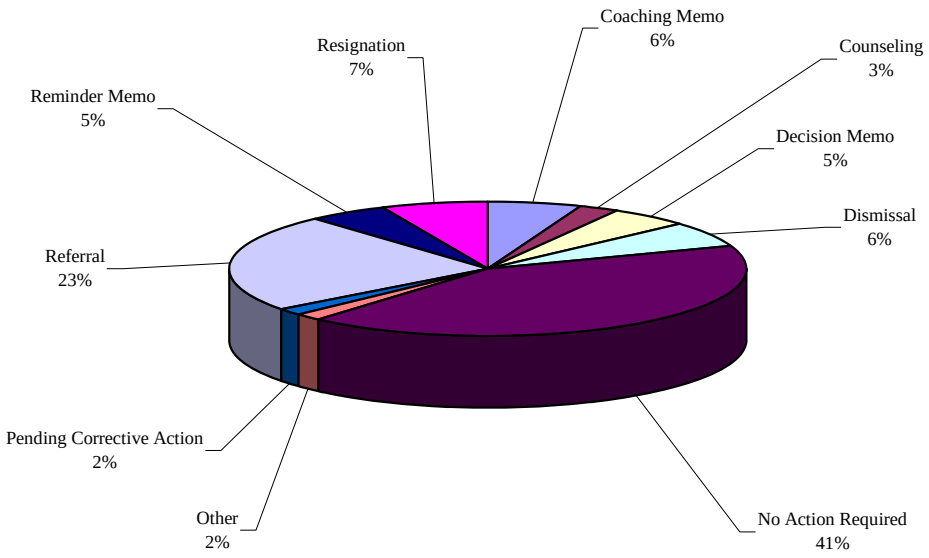
Unauthorized Use of State Equipment/Confidentiality/Violation of State Tax Law

The OIG received information that an employee was using state equipment in association with his personal business. The employee admitted to answering his work telephone by using the name of his business, using the printer and Internet to check his business bank account and to apply for a business loan. Also, a review of the employee's work e-mail account indicated that the employee sent confidential information without using the required secured e-mail for transmitting confidential tax information. The employee also failed to comply with state tax law concerning his private business. The employee was dismissed from Revenue.

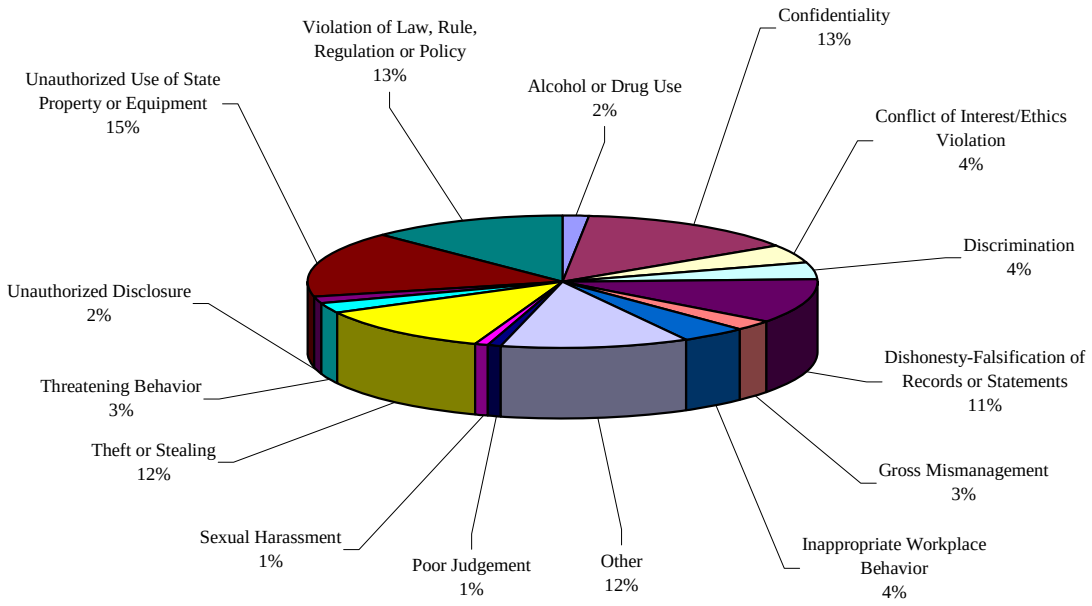
Unauthorized Use of State Equipment
The OIG received information that an employee was sending inappropriate emails to co-workers. The employee admitted to sending e-mails which contained sexual or racial overtones and at least one inappropriate e-mail attachment to co-workers using his state-owned computer. The employee stated that the bulk of the emails was sent to one particular employee. The employee was disciplined.

Unauthorized Use of State Equipment
The OIG received information that an employee spent an excessive amount of time chatting on Instant Messenger (IM). The Internet history revealed that the employee was in chat sessions the majority of her workday, listening to music and/or watching a movie. Office rumors indicated that the employee brought her personal external hard drive to work daily and connected it to her assigned state-owned computer. The employee admitted to the allegations and subsequently resigned from her position.

Cases Closed by Final Disposition



Cases Closed by Type



Summary of Closed Cases:

Project Number	Disposition	Type
06258	Unsubstantiated	Violation of Law, Rule, Regulation or Policy
06491	Unsubstantiated	Inappropriate Workplace Behavior
07125	Substantiated	Violation of Law, Rule, Regulation or Policy
07188	Substantiated	Dishonesty-Falsification of Records or Statements
07250	Unsubstantiated	Confidentiality
07271	Substantiated	Other
07278	Unsubstantiated	Discrimination
07289	Unsubstantiated	Other
07291	Unsubstantiated	Confidentiality
07339	Referral	Other
07364	Substantiated	Unauthorized Use of State Property or Equipment
07379	Unsubstantiated	Other
07383	Unsubstantiated	Alcohol or Drug Use
07401	Referral	Unauthorized Disclosure
07425	Referral	Theft or Stealing
07426	Referral	Theft or Stealing
07429	Referral	Theft or Stealing
07431	Substantiated	Dishonesty-Falsification of Records or Statements
07442	Unsubstantiated	Theft or Stealing

Project Number	Disposition	Type
07454	Unsubstantiated	Violation of Law, Rule, Regulation or Policy
07456	Substantiated	Theft or Stealing
07474	Substantiated	Inappropriate Workplace Behavior
07481	Unsubstantiated	Violation of Law, Rule, Regulation or Policy
07505	Substantiated	Inappropriate Workplace Behavior
07514	Substantiated	Theft or Stealing
07516	Unsubstantiated	Theft or Stealing
07536	Referral	Unauthorized Use of State Property or Equipment
07538	Referral	Unauthorized Use of State Property or Equipment
07542	Unsubstantiated	Confidentiality
07543	Substantiated	Theft or Stealing
07545	Substantiated	Unauthorized Use of State Property or Equipment
07546	Unsubstantiated	Violation of Law, Rule, Regulation or Policy
07563	Unsubstantiated	Unauthorized Use of State Property or Equipment
07564	Substantiated	Conflict of Interest/Ethics Violation
08007	Substantiated	Violation of Law, Rule, Regulation or Policy
08009	Unsubstantiated	Other
08010	Referral	Unauthorized Use of State Property or Equipment
08011	Unsubstantiated	Theft or Stealing

Project Number	Disposition	Type
08020	Unsubstantiated	Other
08027	Unsubstantiated	Unauthorized Use of State Property or Equipment
08028	Unsubstantiated	Theft or Stealing
08033	Unsubstantiated	Other
08034	Referral	Alcohol or Drug Use
08035	Unsubstantiated	Other
08044	Unsubstantiated	Threatening Behavior
08045	Substantiated	Conflict of Interest/Ethics Violation
08053	Unsubstantiated	Other
08057	Unsubstantiated	Discrimination
08058	Unsubstantiated	Gross Mismanagement
08065	Referral	Unauthorized Use of State Property or Equipment
08098	Unsubstantiated	Discrimination
08099	Unsubstantiated	Confidentiality
08101	Substantiated	Unauthorized Use of State Property or Equipment
08111	Referral	Dishonesty-Falsification of Records or Statements
08114	Unsubstantiated	Other
08117	Substantiated	Confidentiality
08118	Referral	Unauthorized Use of State Property or Equipment

Project Number	Disposition	Type
08119	Unsubstantiated	Other
08125	Substantiated	Unauthorized Use of State Property or Equipment
08126	Substantiated	Unauthorized Use of State Property or Equipment
08127	Substantiated	Sexual Harassment
08137	Referral	Gross Mismanagement
08138	Unsubstantiated	Unauthorized Use of State Property or Equipment
08139	Unsubstantiated	Theft or Stealing
08150	Unsubstantiated	Theft or Stealing
08151	Referral	Other
08162	Referral	Dishonesty-Falsification of Records or Statements
08169	Substantiated	Violation of Law, Rule, Regulation or Policy
08172	Unsubstantiated	Violation of Law, Rule, Regulation or Policy
08180	Substantiated	Confidentiality
08181	Substantiated	Unauthorized Use of State Property or Equipment
08190	Unsubstantiated	Discrimination
08192	Substantiated	Confidentiality
08193	Referral	Dishonesty-Falsification of Records or Statements
08194	Substantiated	Unauthorized Use of State Property or Equipment
08202	Unsubstantiated	Dishonesty-Falsification of Records or Statements

Project Number	Disposition	Type
08220	Unsubstantiated	Theft or Stealing
08222	Unsubstantiated	Confidentiality
08224	Unsubstantiated	Dishonesty-Falsification of Records or Statements
08227	Substantiated	Unauthorized Use of State Property or Equipment
08228	Unsubstantiated	Confidentiality
08240	Referral	Other
08246	Substantiated	Confidentiality
08249	Substantiated	Poor Judgment
08251	Referral	Violation of Law, Rule, Regulation or Policy
08252	Unsubstantiated	Dishonesty-Falsification of Records or Statements
08253	Unsubstantiated	Gross Mismanagement
08265	Substantiated	Dishonesty-Falsification of Records or Statements
08283	Substantiated	Unauthorized Use of State Property or Equipment
08284	Substantiated	Confidentiality
08290	Unsubstantiated	Inappropriate Workplace Behavior
08307	Unsubstantiated	Dishonesty-Falsification of Records or Statements
08329	Unsubstantiated	Confidentiality
08345	Substantiated	Violation of Law, Rule, Regulation or Policy
08371	Unsubstantiated	Confidentiality

Project Number	Disposition	Type
08379	Substantiated	Confidentiality
08380	Unsubstantiated	Dishonesty-Falsification of Records or Statements
08381	Substantiated	Unauthorized Use of State Property or Equipment
08387	Unsubstantiated	Other
08390	Referral	Conflict of Interest/Ethics Violation
08395	Referral	Conflict of Interest/Ethics Violation
08397	Unsubstantiated	Confidentiality
08404	Referral	Violation of Law, Rule, Regulation or Policy
08413	Substantiated	Dishonesty-Falsification of Records or Statements
08422	Substantiated	Inappropriate Workplace Behavior
08439	Substantiated	Unauthorized Use of State Property or Equipment
08440	Referral	Dishonesty-Falsification of Records or Statements
08458	Substantiated	Violation of Law, Rule, Regulation or Policy
08460	Substantiated	Violation of Law, Rule, Regulation or Policy
08461	Unsubstantiated	Violation of Law, Rule, Regulation or Policy
08465	Unsubstantiated	Threatening Behavior
08466	Substantiated	Confidentiality
08467	Substantiated	Confidentiality
08471	Referral	Violation of Law, Rule, Regulation or Policy

Project Number	Disposition	Type
08549	Referral	Conflict of Interest/Ethics Violation
08575	Unsubstantiated	Discrimination
08587	Substantiated	Theft or Stealing
08601	Unsubstantiated	Threatening Behavior
08603	Substantiated	Unauthorized Disclosure

Security and Disclosure Section

Revenue's Security and Disclosure Officer supervises the Security and Disclosure Section (SDS) of the OIG. The SDS is assigned various responsibilities related to the security of Revenue's property, equipment, information, and personnel. These responsibilities include programs related to:

- Physical security, including employee photo identification.
- Workplace violence, including: assaults and threats from external customers, domestic violence affecting the workplace, and incidents of violent behavior between employees.
- Emergency management, including coordinating the development and maintenance of Revenue's Continuity of Operations Plan (COOP).
- Criminal history record checks on employees.
- Disclosure and information sharing between federal, state and local governments.
- Discrimination and sexual harassment complaint intake.

The goals of the SDS are to provide a safe and secure work environment for Revenue employees, safeguard confidential information from unauthorized use or disclosure, protect department-owned equipment against theft and/or vandalism, and provide management with information necessary to ensure a desired level of integrity among department staff.

Security and Disclosure Section Accomplishments During FY 2008/09

- Worked with ISP to further enhance the agency's Information Security Awareness Program.
- Revised Revenue's Continuity of Operations Plan (COOP) and submitted to the Division of Emergency Management for approval.
- Coordinated development of a comprehensive Department Emergency Management Policy.
- Developed and facilitated the second annual tabletop hurricane exercise for Revenue managers.
- Streamlined the Security Review Report process to provide more relevant and timely information to managers.
- Incorporated reporting requirements in Revenue's Standards of Conduct for an employee named as respondent in domestic violence injunctions.
- Revised Revenue's policy on weapons in the workplace within the Standards of Conduct.
- Clarified reporting requirements within the Standards of Conduct for employees arrested or charged with criminal offenses.
- Established requirements within the Standards of Conduct for employees to report driver's license suspensions and revocations.
- Established requirements within the Standards of Conduct for employees to resolve and report resolution of outstanding arrest warrants.

Workplace Security

Three SDS staff members possess the designation of Florida Crime Prevention Practitioner and four SDS staff members possess the designation of Florida Crime Prevention Through Environmental Design (CPTED) Practitioner. The Office of the Attorney General awards these designations after completion of courses offered by the Florida Crime Prevention Training Institute.

Personal and physical security standards using CPTED techniques and concepts have been established in the "model office" concept and are used both in the design of new facilities and during on-site security reviews of Revenue facilities. During FY 2008/09, the SDS reviewed proposed floor plans of new facilities and worked with facilities management to implement the "model office" concept in new and renewed leases.

During FY 2008/09, SDS staff conducted on-site security surveys of Revenue offices at the following locations:

Location	Program	Date Completed
Gainesville	CSE	07/07/2008
Alachua	GTA	07/07/2008
Leesburg	CSE	07/08/2008
Leesburg	GTA	07/08/2008
Cocoa	CSE	07/09/2008
Cocoa	GTA	07/09/2008
Okeechobee	CSE	07/10/2008
Vero Beach	CSE	07/10/2008
Sebring	CSE	07/11/2008
Kissimmee	CSE	07/11/2008
Chipley	CSE	08/14/2008
Quincy	CSE	08/14/2008
Key West	CSE	11/18/2008
Key West	GTA	11/18/2008
Miami	GTA	11/19/2008
Naples	CSE	11/20/2008
Naples	GTA	11/20/2008
Tallahassee	CSE	06/18/2009
Tallahassee	GTA	06/18/2009

The objective of these reviews is to evaluate the facilities to identify potential security risks and assess the existing levels of protection for Revenue personnel, equipment, and information. In addition to assessing security issues specific to Revenue, the OIG security survey checklist captures information to meet statutory reporting requirements of s. 943.0311, F.S., the Homeland Security Comprehensive Assessment Model (HLS-CAM) Vulnerability Assessment. Recommendations were made to management to reduce or eliminate potential security risks to Revenue employees, equipment, and information.

Revenue Employee Identification Card System

The SDS administers Revenue's employee identification card system, which is integrated with a proximity card based access control system for Revenue facilities located in Tallahassee, Florida. With the exception of one Revenue office located in the Northwood Center complex, all Revenue facilities in Tallahassee are currently using the access control system maintained by the SDS. In FY 2008/09, the SDS processed 1,951 requests for access and/or photo identification cards.

Workplace Violence

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

Workplace violence can originate from internal or external sources. Most reported workplace violence incidents are from external sources. External workplace violence incidents include assaults and threats made against any Revenue employee as a result of their official duties. External-sourced workplace violence also includes threats made to Revenue by a customer or client but directed toward someone else, such as a noncustodial parent in a child support case threatening to harm the custodial parent in the case or altercations between clients while on Revenue property.

Threats of suicide made by clients or customers to Revenue employees are reported to and logged by the SDS as external workplace violence incidents. Response may include notifying local law enforcement in the area where the person making the threat lives and requesting that they perform a wellness check.

Internal workplace violence incidents are generally addressed by assembling Revenue's Workplace Violence (WPV) Team. The WPV Team consists of the Inspector General, the Security and Disclosure Officer, the Employee Relations Manager, and the Attorney Supervisor for Administrative Services in the Office of General Counsel. The 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.

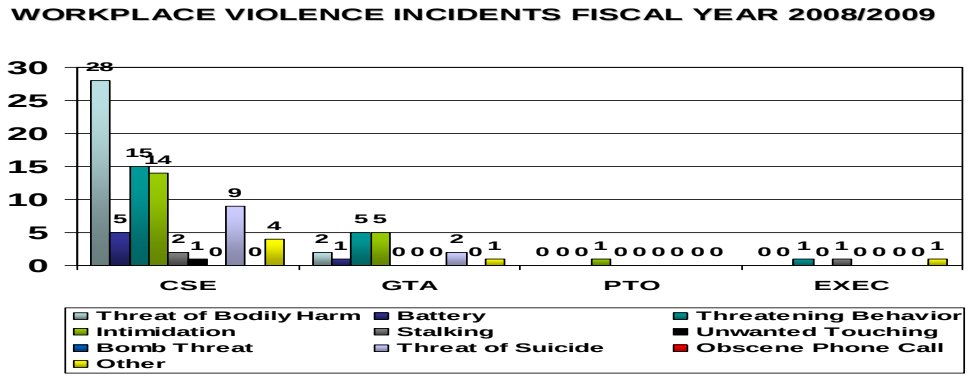
Domestic violence affecting the workplace is a primary concern. Domestic violence could be initiated by an external or internal source. Revenue's Standards of Conduct were revised in November 2008 to require any employee who is named as the respondent in an injunction for protection against domestic violence, or any similar injunction, to report the injunction to the Office of Inspector General. The SDS 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 also be convened to address more serious incidents of domestic violence affecting the workplace.

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 any employee that a PDC is associated with the case and special care should be taken in any contact or action on this account. SDS 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 responsibilities are carried out in relation to a PDC account.

A total of 98 reports of actual or potential workplace violence were received during FY 2008/09, down slightly from the 118 incidents reported during the previous fiscal year. Only two of these incidents involved a Revenue employee as the perpetrator and nine incidents of domestic violence potentially affecting the workplace were reported. CSE reported 78 incidents, GTA reported 16 incidents, the Property Tax Oversight (PTO) Program reported one incident, and the Executive Support (EXEC) Program reported one incident. No incidents were reported by ASP or ISP

The graph below depicts the types of incidents received by program:



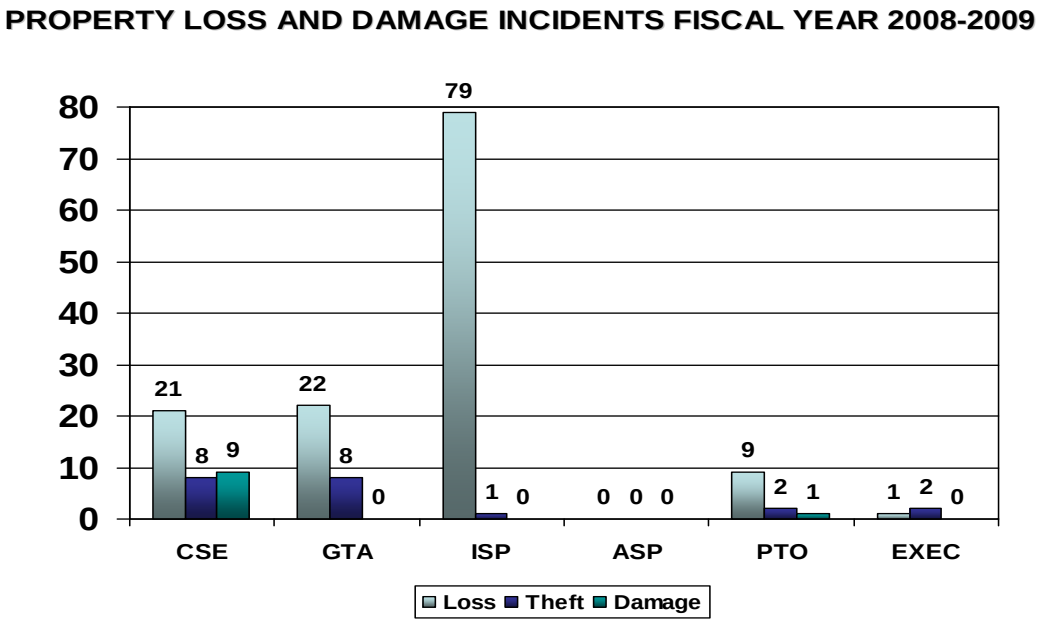
The SDS continually seeks out methods and strategies to combat workplace violence and apply them in our day-to-day activities.

Property Loss and Damage

Policies require the reporting of any theft, loss, or damage of Revenue owned property to the OIG. Employees are encouraged to report loss or vandalism of personally owned property that occurs at the workplace, but it is not required. The SDS tracks property loss and damage reports to identify problem areas or weaknesses in security controls, allowing us to determine where improvements are needed in security procedures to better protect Revenue's assets.

A total of 164 property loss or damage incidents were reported during FY 200/09. This was a significant increase over the 43 incidents reported in FY 2007/08. The increase can primarily be attributed to the implementation of Ethics Link, Revenue's new, centralized on-line reporting tool for all internal incidents, concerns, or complaints; which directs all property loss reports to the OIG, including reports of property that is identified as missing during the annual property inventory process. CSE reported 39 incidents, GTA reported 30 incidents, ISP reported 80 incidents, PTO reported 12 incidents, and EXEC reported three incidents. No property losses were reported by ASP during the fiscal year.

The graph below depicts the types of incidents received for FY 2008/09, by program:



Emergency Management

The Security and Disclosure Officer is designated as the Emergency Coordinating Officer (ECO) for the agency. As required by s. 252.365, F.S., this position is responsible for ensuring the agency has a disaster preparedness plan. In this capacity, the SDS maintains Revenue's COOP and is responsible for updating, testing, and implementing the plan. During the year, the SDS staff worked with senior management to revise Revenue's COOP to make it an all-hazards-type plan. The plan addresses both natural and man-made threats including influenza pandemics, hurricanes, weapons of mass destruction, building fires, civil disturbances, and any other threats to Revenue's staff and/or facilities. The revised plan was sent to the Division of Emergency Management for approval.

During the year, SDS staff worked with executive management to establish a comprehensive Emergency Management Policy. The policy addresses implementation of COOP, documentation of the Executive Director's authority to waive rules when needed to respond to an emergency, delegations of authority, and provisions for the closing of Revenue offices due to emergencies.

SDS staff also coordinates Revenue's participation in the operation of the Florida Emergency Information Line (FEIL). During disaster activations of the State Emergency Operations Center, FEIL will be activated and staffed by teams from state agencies on a rotating basis. Revenue has 2 teams of 24 staff members, each trained and ready for activation during the hurricane season.

During activations of the State Emergency Operations Center, SDS staff represents Revenue in Emergency Support Function (ESF) 18, Economic Stabilization. ESF 18 coordinates with state

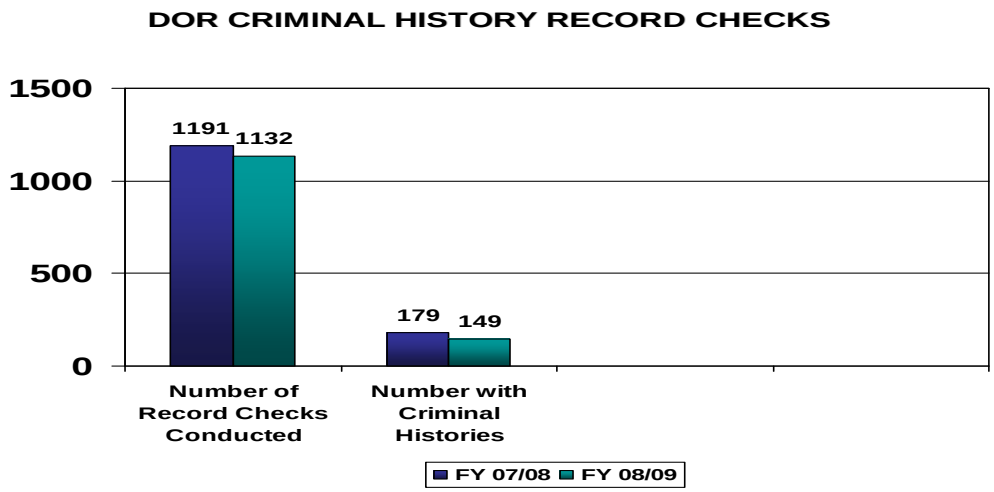
and federal agencies to assist local organizations providing financial, unemployment, and technical resources needed to restore business operations after a disaster. An SDS employee was designated as the acting ESF 18 ECO for the latter half of the fiscal year, which involved coordination of all ESF 18 activities.

Criminal History Record Checks

The SDS is responsible for performing criminal history record checks of Revenue employees. All new employees, including Other Personal Services (OPS), must have a national criminal history record check conducted upon initial employment. This record check requires the submission of fingerprints to the Federal Bureau of Investigations (FBI) through the Florida Department of Law Enforcement (FDLE).

All employees are subject to an updated criminal history record check when they experience a change in appointment and it has been more than one year from the date of their initial or last criminal history record check. Employees who work and reside within the state of Florida are subject only to a Florida criminal history record check through FDLE. To promote cost-effectiveness and reduce the burden of conducting multiple state criminal history record checks, a national criminal history record check is conducted on employees who reside or work outside the state of Florida any time a record check is required.

The graph below reflects the number of criminal history record checks conducted and criminal histories identified for the past two fiscal years:



Criminal History Follow-Up Reviews

When reports are received from FDLE or the FBI indicating arrests or convictions, a criminal history follow-up review is opened in the SDS. During the follow-up review process, the necessary court records and other documentation are obtained to determine or verify final disposition of charges. Employment applications are then compared to court documentation to determine if background information questions were accurately completed.

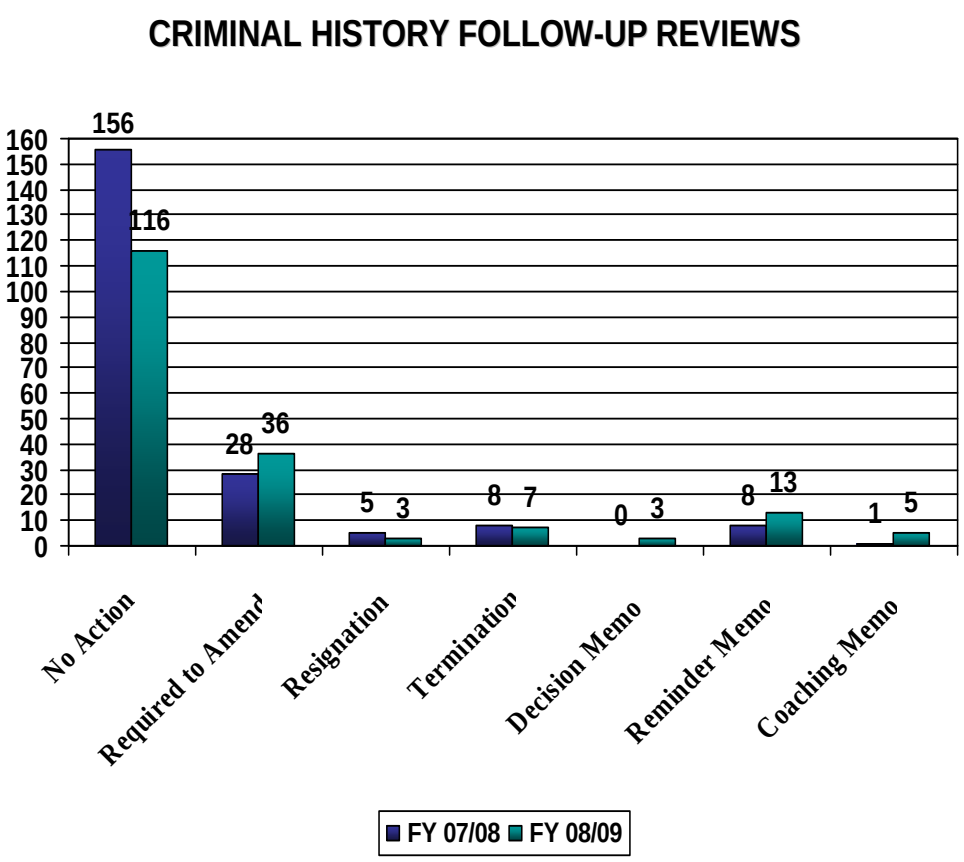
The SDS also opens criminal history follow-up reviews when information is obtained from the employee or other sources regarding criminal offenses that were not identified by FDLE or FBI criminal history reports.

If a first-degree misdemeanor or felony is not accurately reflected on the employment application, a report of findings is forwarded to the appropriate program management who, in consultation with the Human Resource Services Process (HRSP) and OGC staff, determines and initiates appropriate corrective actions. The standard proposed action for providing false information is termination; however, management may, in consultation with HRSP and OGC staff, determine if using Revenue's established mitigation criteria is appropriate. If mitigated, an employee may receive corrective measures ranging from no action taken to a decision memo.

If an offense is less than a first-degree misdemeanor or felony, or the employee accurately reflected his or her criminal history on the employment application, the review is closed with no action. If it is determined that an employee made a valid attempt to be truthful in reflecting criminal history information but the Background Information section of the State of Florida Employment Application did not contain complete, current, and accurate information, a request is submitted to HRSP to obtain an amended employment application from the employee that accurately reflects the employee's background information.

The SDS stresses the importance of accurately completing background information questions on the state employment application. Revenue supervisors are required to specifically discuss the background information section of the employment application during the interview process and applicants are given the opportunity to make changes to their applications, if necessary. This communication is documented by use of the "Background Information Verification Form" completed by each interviewed applicant.

A total of 183 criminal history follow-up reviews were completed during FY 2008/09. The graph below reflects the outcome of criminal history follow-up reviews and reports for the past two years.

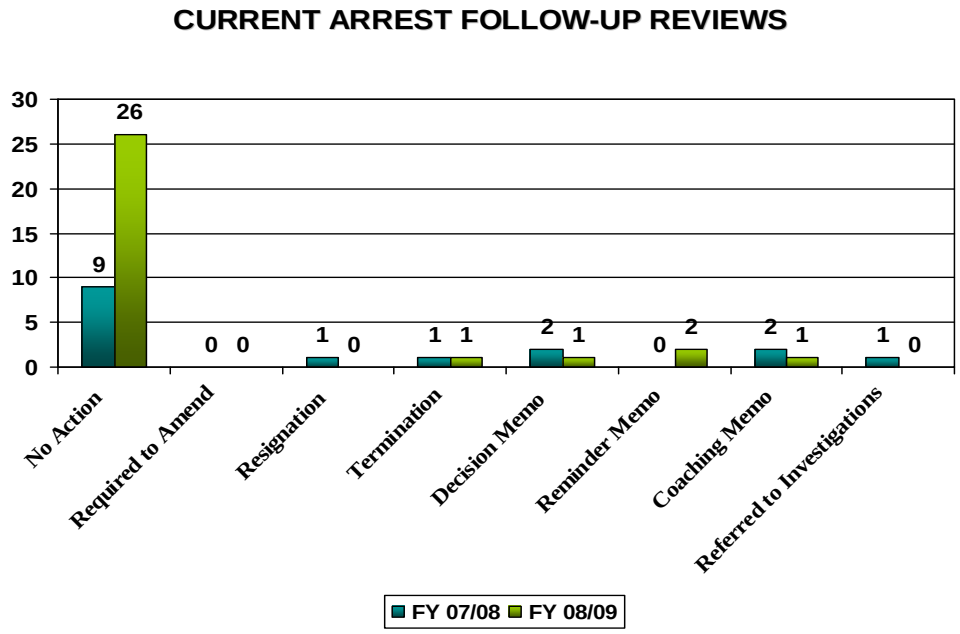


Seventeen criminal history follow-up review cases were open and pending final outcome at the close of the fiscal year.

Employee Arrest Reports

The SDS is also 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 report any arrest and/or charge for a crime that is punishable by more than 60 days imprisonment and/or more than a $500 fine. The employee must also report the final order or other disposition of such an arrest or charge. Twenty-three current arrest follow-up review cases were opened during the fiscal year and 31 reviews were closed.

The graph below reflects the outcome of current arrest follow-up reviews and reports for the past two years.

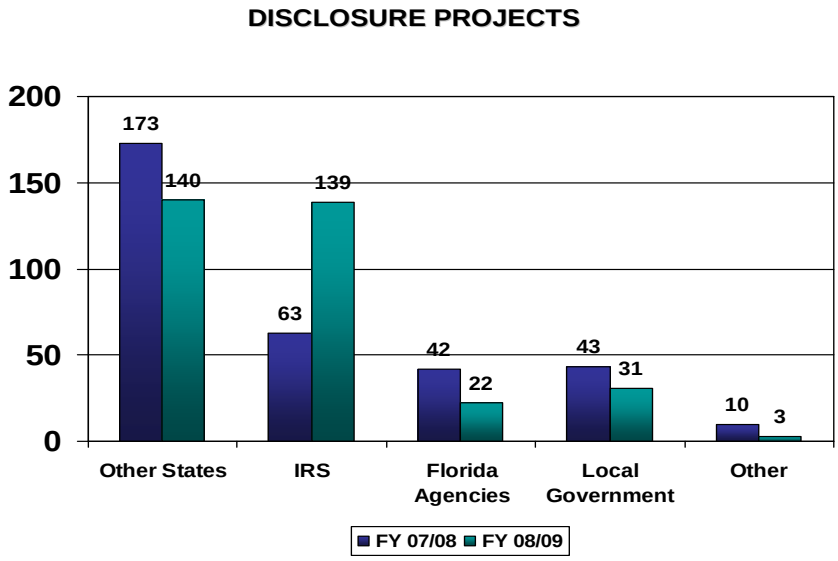


Two current arrest follow-up review cases were open and pending final outcome at the close of the fiscal year.

Disclosure/Information Sharing

Most tax and child support information maintained by Revenue is confidential and specifically exempt from disclosure. Section 213.053, F.S., identifies confidential tax information and provides criminal penalties for the unauthorized use or disclosure of confidential tax information. The statute also provides specific exceptions to the confidentiality law that allow Revenue to share tax information with specified entities, sometimes for specified purposes. As stated in Chapter 12-22, F.A.C, the Security and Disclosure Officer is the delegated authority to disclose confidential information as allowed by statute. The SDS is responsible for coordinating information sharing between Revenue and tax administration agencies in other states, the IRS, other Florida agencies, and local taxing authorities that are authorized by statute to receive confidential state tax information.

The following chart depicts disclosure and information-sharing activity over the past two years:



Other States
Florida makes every effort to assist other states in tax administration and increasing tax compliance rates. In turn, the SDS coordinates requests for information from other states' tax agencies when needed to enhance the administration of Florida tax law. Currently, Revenue has information-sharing agreements with every state's tax administration agency except the state of Nevada. These agreements are either individually with each state or through the Federation of Tax Administrators' Uniform Exchange of Information Agreement. Information is provided to or received from other states in response to specific requests for information on Florida taxpayers or in the form of referrals as allowed by the specific agreements.

Internal Revenue Service (IRS)
The Security and Disclosure Officer is Revenue's liaison with the IRS for information-sharing purposes and continues to work closely with the IRS on various joint projects and information-sharing activities.

Every three years, the IRS conducts an on-site review to ensure Revenue is meeting both the "need and use" requirements and federal requirements for safeguarding federal tax information received in both the tax administration and child support programs. The SDS coordinates and works with the operating programs to prepare for these reviews and respond to any findings or recommendations made by the IRS review teams. During FY 2008/09, preparations began for the IRS Safeguard Review that is scheduled to be conducted in September 2009.

Florida Agencies
We continue to work with other Florida government agencies whenever possible to enhance tax administration and other state programs, within the limitations of disclosure and information-sharing laws relative to tax information. The SDS maintains information-sharing agreements with other Florida agencies required by s. 213.053, F.S.

Local Governments
We provide assistance to county property appraisers, county tax collectors, and other local tax authorities as allowed by law. Assistance may include providing advice on confidentiality issues, responding to requests for state tax information, and acting as a liaison between local governments and other states' tax administration agencies.

Local government coordination includes working with GTA and ISP staff to provide required communications services tax information to authorized local government staff via a secure Internet site.

SDS staff assists in the administration of the Revenue Information Sharing and Exchange (RISE) program, working closely with the GTA RISE Coordinator to promote awareness of confidentiality and safeguard requirements placed on state tax information received through the RISE program. The section also provides guidance to service center employees who work closely with local governments on tourist development tax issues.

SDS staff actively participates on the Revenue Information Security Committee (RISC). RISC was formed to address information security issues that face Revenue on a day-to-day basis. Information security is a primary concern for Revenue due to the confidential nature of child support and tax information, and the criminal penalties associated with unauthorized use or disclosure of this information. Through participation on RISC, SDS staff provides input for all aspects of information disclosure to help ensure an appropriate level of security for Revenue information resources.

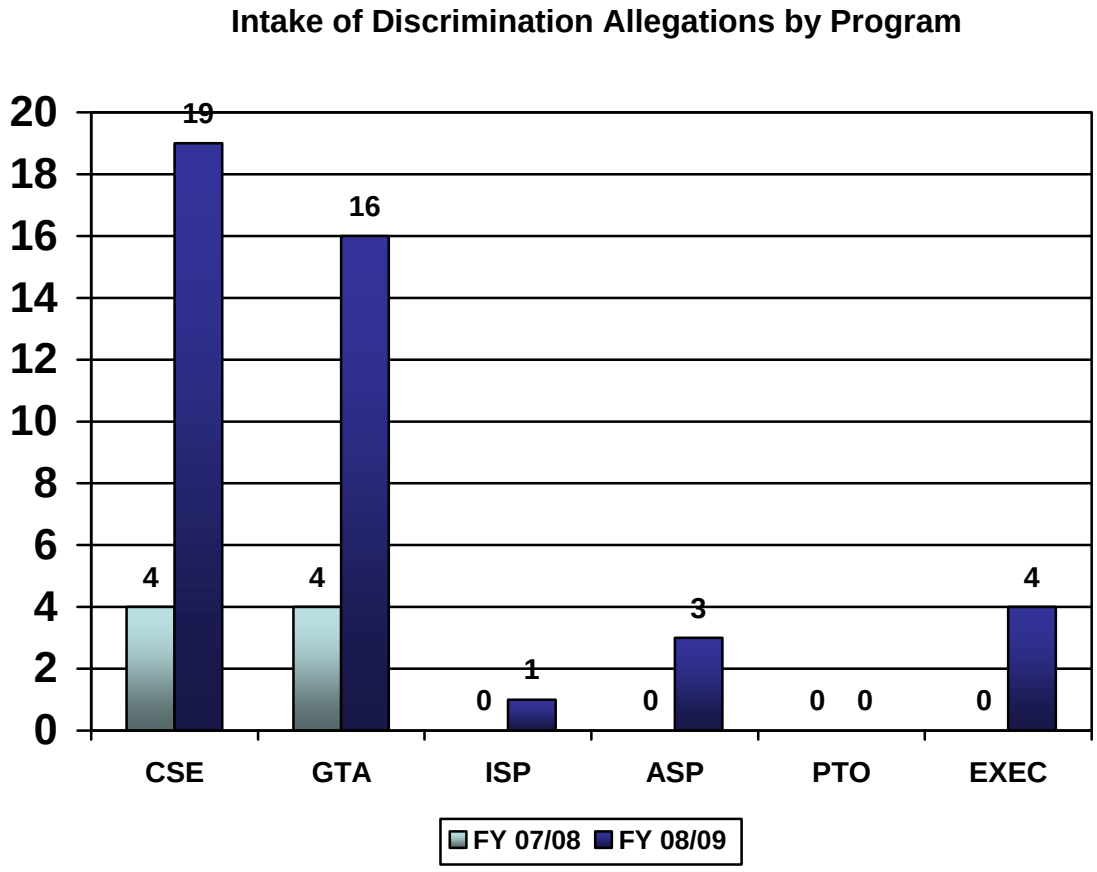
Discrimination and Sexual Harassment Complaint Intake
Intake and preliminary review of discrimination and sexual harassment complaints is assigned to the SDS. The Operations and Management Consultant Manager in the SDS is the Discrimination and Sexual Harassment Intake Officer for Revenue. The intake 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 not be limited to, referral to IIS, referral to management or other entities for corrective or other appropriate action, or no further action may be required.

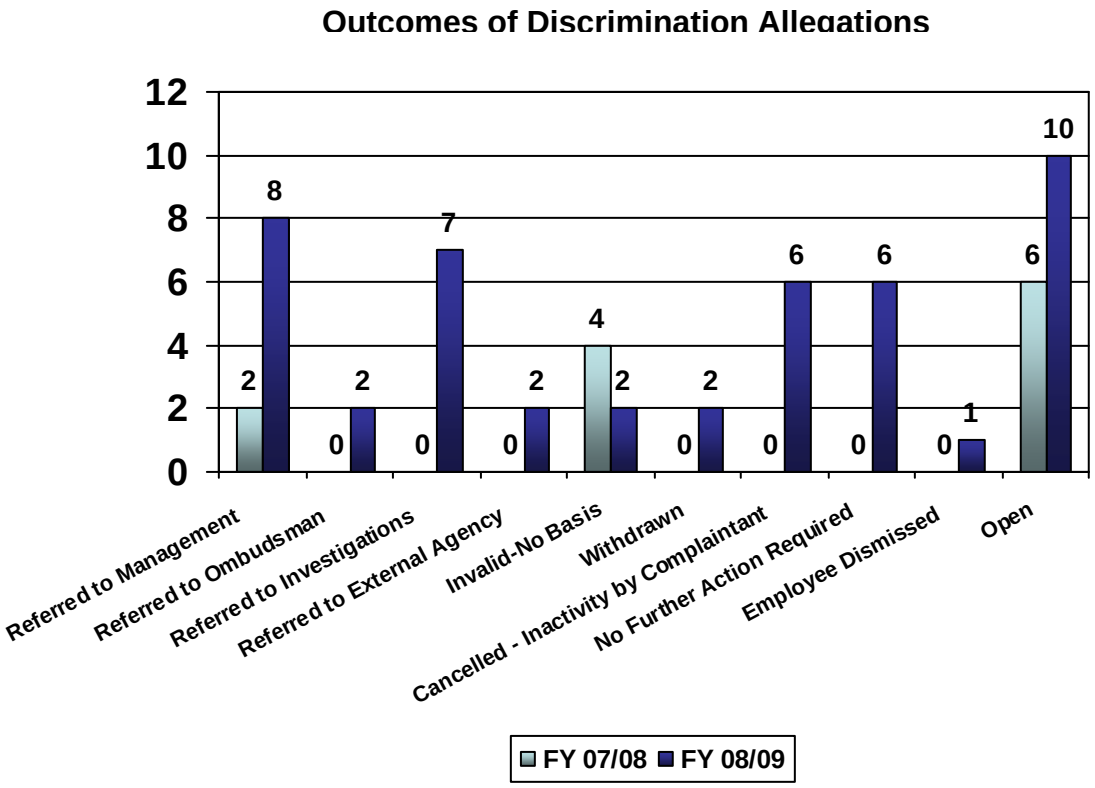
Sexual harassment is a form of sex discrimination under Title VII of the Civil Rights Act of 1964, and s. 760.10, F.S. It is considered "conduct unbecoming a public employee" as provided in s. 110.227, F.S., and "misuse of public position" as provided in s. 112.313, F.S. Revenue policy states that every employee has a right to work in an environment free from any form of discrimination or retaliation against those who oppose or report sexual harassment.

Any employee may seek corrective action and relief from sexual harassment and other forms of discrimination inside the agency without fear of retaliation. Revenue's Sexual Harassment Policy requires any supervisory employee who has actual knowledge of sexual harassment or

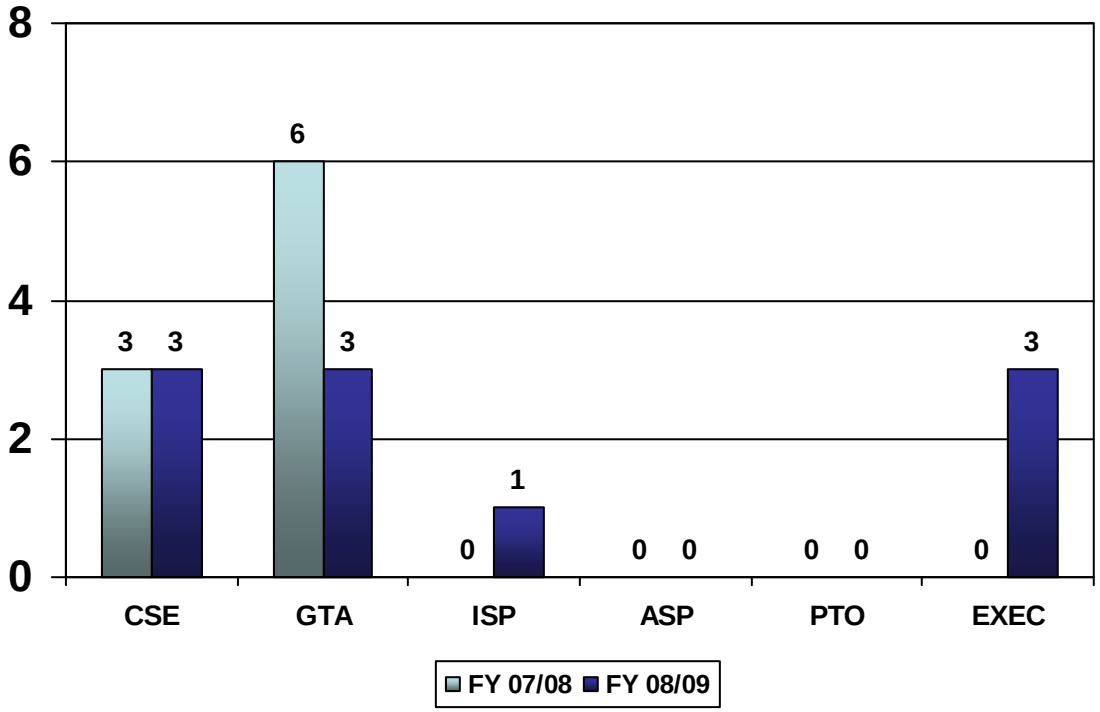
retaliation involving any of the employees he or she supervises, or involving another supervisor or any employee supervised by another, to report the matter directly to the intake officer. Any supervisory employee who fails to report an incident of sexual harassment or retaliation may be subject to corrective action, up to and including dismissal.

The graphs below reflect internal complaints of discrimination and their outcomes for the past two years: During FY 2008/09, intake and review were performed on 43 reports of alleged discrimination or sexual harassment. Ten reports involved allegations of sexual harassment. While sexual harassment is a form of sex discrimination, to provide a more focused review, allegations involving only sexual harassment have been highlighted in additional graphs.

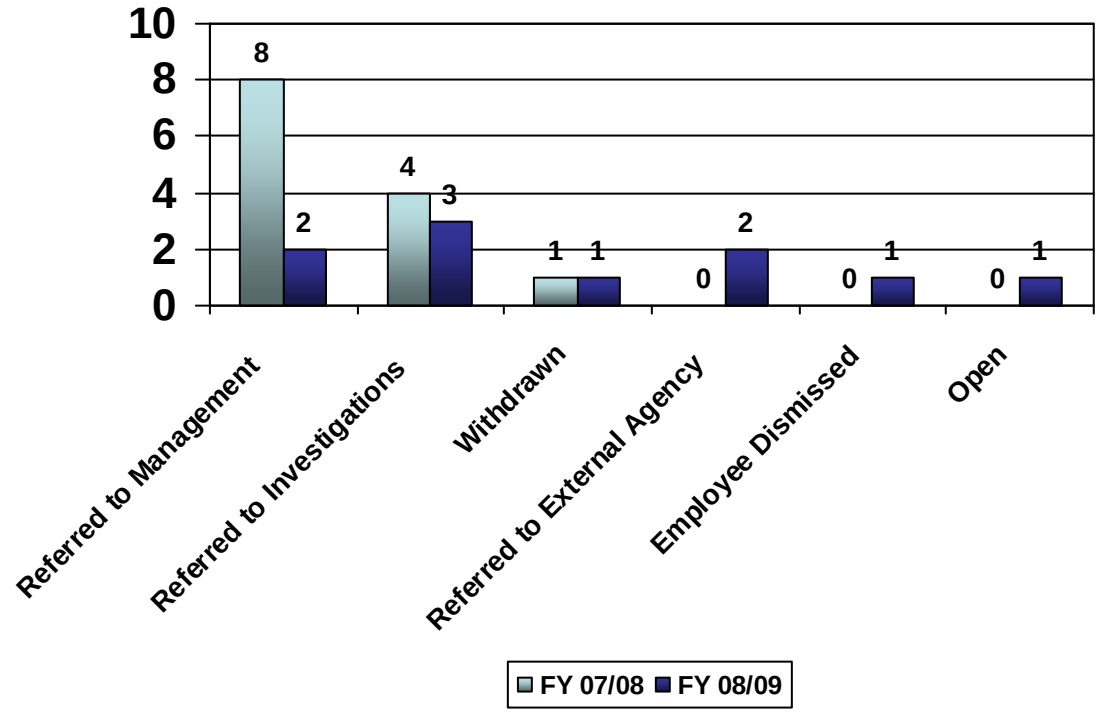



Outcomes of Discrimination Allegations
12
10
8
6
4
2
0
2
8
0
2
0
7
0
2
4
2
0
2
0
6
0
6
0
1
6
10
Referred to Management
Referred to Ombudsman
Referred to Investigations
Referred to External Agency
Invalid-No Basis
Withdrawn
Cancelled - Inactivity by Complaintant
No Further Action Required
Employee Dismissed
Open
FY 07/08
FY 08/09

Intake of Sexual Harassment Allegations



Outcomes of Sexual Harassment Allegations



The three cases referred to IIS involved three separate reports of inappropriate behavior by an employee who allegedly continued to repeat acts of inappropriate workplace behavior after receiving instruction regarding expected standards of behavior in the workplace. The cases were referred to determine if the alleged repeated behavior was sufficiently pervasive or severe to have the purpose or effect of unreasonably interfering with an individual's work performance, or creating an intimidating, hostile or offensive working environment to constitute sexual harassment under the law.

The case resulting in dismissal involved an employee who had been the subject of a sexual harassment complaint in 2006. In both cases, allegations were brought forward by the employee's girlfriends, who were also Revenue employees. Both cases involved domestic violence and anger management issues. While reviewing the current year's allegations, it was discovered the employee had been charged with domestic violence and was the subject of a protection order in 2007 involving another female who was not a Revenue employee. After the employee's October 2008 domestic violence event, he failed to return to work and was dismissed during the probationary period of his current position.

Generally, cases referred to program management involve allegations that are insufficient to constitute sexual harassment and require a manager to address incidents of inappropriate workplace behavior in accordance with Revenue's Standards of Conduct. Cases referred to IIS possess the necessary prima facie elements, if proven factual, to support a formal charge of discrimination through the Equal Employment Opportunity Commission (EEOC) or the Florida Commission on Human Relations (FCHR).

During FY 2008/09, five employees who participated in Revenue's Discrimination and Sexual Harassment Intake Process also filed external charges of discrimination with the EEOC or the FCHR. Three of the five had their internal and external complaints closed without a finding of unlawful employment discrimination and two remained open with the EEOC or FCHR.

Get Lean Hotline

The Operations and Management Consultant Manager in the SDS also serves as the intake and initial review point for Get Lean Hotline information. The Get Lean Hotline was established by the State's Chief Financial Officer to provide a mechanism for receiving information and suggestions from the citizens of the state of Florida on how to improve the operation of government, increase governmental efficiency, and eliminate waste in government.

In August 2008, responsibility for intake of Get Lean Hotline Complaints was transferred to the IIS. Up to that point, there were no Get Lean Hotline complaints forwarded to Revenue and there were no complaints received during the previous fiscal year.

Safety and Loss Prevention Program

The Safety and Loss Prevention Program is designed to provide a safe and healthy work environment. Policies and procedures were developed to formally demonstrate Revenue's commitment to providing a safe and secure workplace for its employees and the citizens of Florida. Revenue demonstrates the value of concern for others by creating the expectation that all employees will maintain a work and business environment that promotes the safety and security of employees and citizens. The Safety Coordinator is responsible for managing Revenue's Safety and Loss Prevention Program. These responsibilities include:

- Coordinating regular and periodic completion of facility and equipment safety inspections of department-operated facilities.
- Compiling Revenue's annual report on loss prevention to the Office of the Governor.
- Compiling the Division of Risk Management's annual safety evaluation report.
- Coordinating training for all employees.
- Developing, applying, and monitoring the Safety and Loss Prevention Program.
- Maintaining copies of records and reports regarding all work-related safety and loss prevention issues for Revenue.
- Providing technical assistance.
- Serving as Revenue's representative on the Interagency Advisory Council on Loss Prevention and as the Chairperson of the Department's Safety Advisory Board.

The degree of success of the Safety and Loss Prevention Program depends largely on support from upper management. Without the support of upper management, supervisors and employees are not likely to support and become involved in the safety program. During FY 2008/09, Revenue held its Second Annual Health and Safety Fair. The Safety Office, Human Resource Services Process, and the Office of Recognition and Community Services coordinated this event. The fair was held at three locations which provided all Tallahassee employees an opportunity to attend.

Revenue was presented the Silver Award by the Interagency Advisory Council on Loss Prevention on May 13, 2009. This award recognizes the recipient's dedicated efforts in loss prevention through an objective comparison of the recipient's safety program to established best practices in loss prevention. The recipient of this award is recognized by the Interagency Advisory Council on Loss Prevention as having a safety program that far exceeds minimum standards for recognition for 2008.

The Safety Office continues to promote Safety Awareness by providing monthly safety posters, safety tips, and/or safety articles. Section 284.50(1)(b), F.S., requires Revenue to perform regular and periodic facility and equipment inspections. The SDS performs office inspections during management reviews. Employees are encouraged to participate and identify safety hazards on a daily basis. All activities were completed solely by in-house personnel and without an allocated budget.

Department of Revenue
Office of Inspector General
P.O. Box 37372
Tallahassee, Florida 32315-7372
(850) 488-4328
INSPGEN@dor.state.fl.us