

***Department of Management Services
Office of Inspector General***

Annual Report for Fiscal Year 2023-2024



September 25, 2024

Pedro Allende
Secretary

Steven Meredith
Interim Inspector General



Office of Inspector General
4030 Esplanade Way, Suite 250
Tallahassee, FL 32399-0950
850-488-5285

Ron DeSantis, Governor
Pedro Allende, Secretary

September 25, 2024

Pedro Allende, Secretary
Department of Management Services
4050 Esplanade Way
Tallahassee, Florida, 32399-0950

Melinda Miguel, Chief Inspector General
Executive Office of the Governor
1902 The Capitol
Tallahassee, Florida 32399-0001

Dear Secretary Allende and Chief Inspector General Miguel:

In accordance with § 20.055, Florida Statutes, I am pleased to present the Annual Report for the Office of Inspector General (OIG). This report reflects the activities and accomplishments of the OIG for Fiscal Year 2023-2024.

We remain committed to the goals of the Department of Management Services and to our work to provide a central point for coordination of and responsibility for activities that promote accountability, integrity, and efficiency.

If you have any questions or require additional information, please contact me. Thank you for your continued support of our efforts.

Respectfully submitted,

A handwritten signature in purple ink, appearing to read "S. Meredith", is written over the typed name below.

Steven Meredith, CPA, CIA, CIGA, CISA, CIG, CIGI
Interim Inspector General

SM/tam

Table of Contents

Introduction	1
Mission Statement	1
Duties and Responsibilities	1
Independence	2
Professional Standards and Code of Ethics	2
OIG Organizational Structure and Staffing	2
Investigative Activity.....	4
Internal Audit Activity	7
Oversight Activities	11
Appendix A: Outstanding Recommendations	14

Introduction

An Office of Inspector General (OIG) is established in each state agency to provide a central point for coordination of, and responsibility for, activities that promote accountability, integrity, and efficiency in government. Section 20.055, Florida Statutes (F.S.), defines the duties and responsibilities of agency inspectors general. The statute requires that the OIG submit an annual report, no later than September 30 of each year, summarizing the office activities during the preceding state fiscal year. This report includes:

- 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 the 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 for which corrective action has not been completed.
- A summary of each audit and investigation completed during the reporting period.

To comply with statutory requirements and to provide Department staff and interested parties with information on OIG progress in accomplishing its mission, this annual report is presented to the Secretary of the Department of Management Services (Department) and the Executive Office of the Governor Chief Inspector General.

Mission Statement

The mission of the OIG is to promote effectiveness, efficiency, and quality within the Department. The OIG provides independent reviews, assessments, and investigations of Department programs, activities, and functions to assist the Department in accomplishing its overall mission. Additionally, the OIG offers consulting services to assist management in their efforts to maximize effectiveness and efficiency.

Duties and Responsibilities

Section 20.055, F.S., outlines the following OIG duties and responsibilities:

- Advise in the development of performance measures, standards, and procedures for the evaluation of state agency programs.
- Assess the reliability and validity of the information provided by the state agency on performance measures and standards, and make recommendations for improvement, if necessary, before submission of such information pursuant to § 216.1827, F.S.
- Review the actions taken by the state agency to improve program performance and meet program standards and make recommendations for improvement, if necessary.
- Provide direction for, supervise and coordinate audits, investigations and management reviews relating to the programs and operations of the state agency.
- Conduct, supervise or coordinate other activities carried out or financed by the agency for the purpose of promoting economy and efficiency in the administration of, or preventing and detecting fraud and abuse in, its programs and operations.

- Keep the Chief Inspector General and Department Secretary informed concerning fraud, abuses, and deficiencies relating to programs and operations administered or financed by the agency, recommend corrective action concerning fraud, abuses, and deficiencies, and report on the progress made in implementing corrective action.
- Ensure effective coordination and cooperation between the Auditor General, federal auditors, and other governmental bodies with a view toward avoiding duplication.
- Review, as appropriate, rules relating to the program and operations of the agency and make recommendations concerning their impact.
- Ensure that an appropriate balance is maintained between audit, investigative, and other accountability activities.
- Comply with *Principles and Standards for Offices of Inspector General* as published and revised by the Association of Inspectors General.

Independence

In accordance with § 20.055(3), F.S., the Inspector General shall be under the general supervision of the agency head for administrative purposes, shall report to the Chief Inspector General, and may hire and remove staff within the Office of Inspector General in consultation with the Chief Inspector General, but independently of the Department. The organizational independence of the Inspector General helps to ensure that audits, investigations, and other activities are performed independently.

Pursuant to state statute, the OIG has full, free, and unrestricted access to all Department activities, records, data, properties, functions, and personnel necessary to effectively carry out its responsibilities.

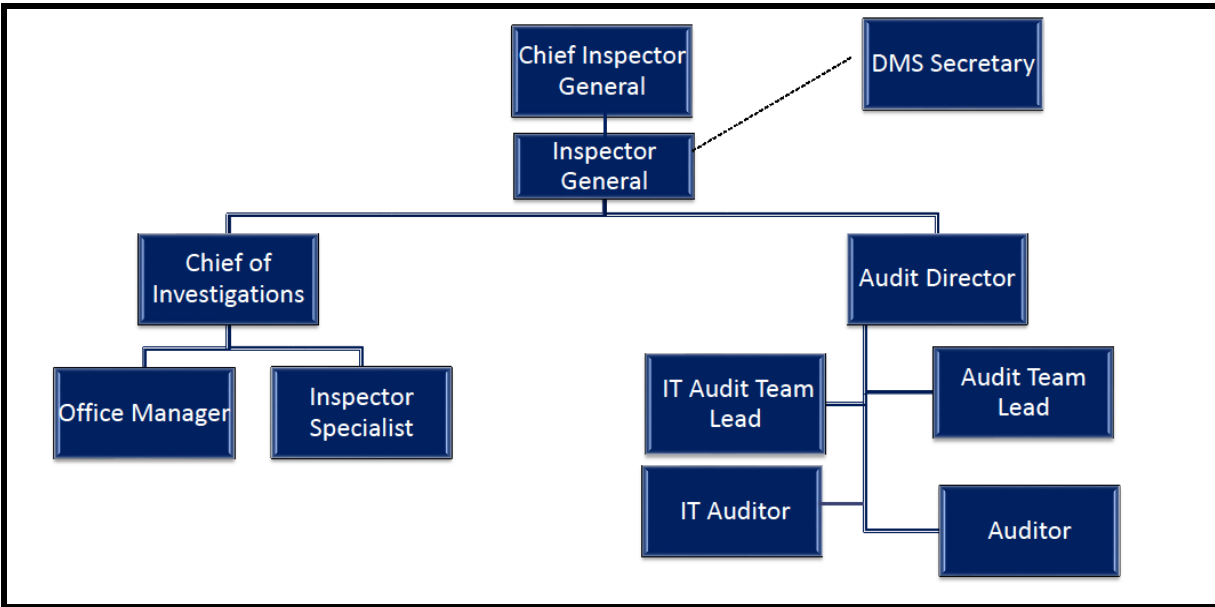
Professional Standards and Code of Ethics

Pursuant to § 20.055, F.S., the OIG complies with *Principles and Standards for Offices of Inspector General* as published and revised by the Association of Inspectors General. Staff abide by the *Florida Code of Ethics for Public Officers and Employees* as codified in § 112.311-112.326, F.S., the Executive Office of the Governor's Code of Ethics, and Department Administrative Policy HR 07-105, *Code of Ethics*. Internal audits are conducted in accordance with *International Standards for the Professional Practice of Internal Auditing (Standards)* and the *Code of Ethics* as published by the Institute of Internal Auditors, Inc.

OIG Organizational Structure and Staffing

The OIG consists of the Inspector General and nine staff positions. The OIG is organized into two sections: Investigations and Internal Audit. The OIG's organizational structure as of June 30, 2023, is shown in Figure 1.

Figure 1 – OIG Organizational Chart



OIG Staff Qualifications and Certifications

OIG personnel are highly qualified and bring various backgrounds and expertise to the Department. The collective experience spans a variety of disciplines including audit, accounting, contracting, investigations, and information technology.

Professional Certifications and Licenses

OIG staff members continually seek to enhance their abilities and contributions to the office and the Department. Many staff members have obtained certifications or licenses that demonstrate their knowledge, motivation, and commitment to the profession. The accomplishments represent significant time and effort by each staff member, reflecting positively on the individuals as well as the Department. During the fiscal year, OIG staff held numerous certifications and licenses as detailed in Table 1 below.

Table 1 – OIG Professional Certifications and Licenses

Professional Certifications and Licenses	No.
Certified Inspector General (CIG)	2
Certified Inspector General Auditor (CIGA)	4
Certified Inspector General Investigator (CIGI)	3
Certified Inspector General Inspector/Evaluator (CIGE)	2
Certified Internal Auditor (CIA)	1
Certified Information Systems Auditor (CISA)	3
Certified Public Accountant (CPA)	2
Certified Public Manager (CPM)	1
Florida Certified Contract Manager (FCCM)	3
Notary Public	3

Professional Affiliations

OIG staff members participate in several professional organizations to maintain proficiency in their areas of expertise and certification. These associations allow them to establish and advance professional networks and participate in professional development activities. OIG staff members are affiliated with the following professional organizations that support audit and investigation activities:

- Association of Inspectors General (National and Local);
- The Institute of Internal Auditors, Inc. (National and Local);
- Association of Government Accountants (National and Local);
- ISACA (National and Local);
- American Institute of Certified Public Accountants; and
- Florida Society of Certified Public Managers.

Continuing Professional Education

Standards, as published by the Institute of Internal Auditors, Inc. and *Principles and Standards for Offices of Inspector General*, as published by the Association of Inspectors General require internal auditors to maintain professional proficiency through obtaining minimum numbers of hours of continuing professional education. Additionally, OIG staff performing investigations must meet minimum training standards as required by the Commission for Law Enforcement Accreditation, Inc.

OIG personnel complete training each year to improve knowledge and skills in audits and investigations. The OIG staff remains committed to seeking professional excellence through continued training and development to ensure the highest quality of service to our customers.

Investigative Activity

Section 20.055, F.S., details investigative duties of the OIG. The OIG shall initiate, conduct, supervise, and coordinate investigations designed to detect, deter, prevent, and eradicate fraud, waste, mismanagement, misconduct, and other abuses in state government. The OIG is required to:

- Receive complaints and coordinate all activities of the agency as required by the *Whistle-blower's Act*, pursuant to § 112.3187-112.31895, F.S.
- Receive and consider complaints that do not meet the criteria for an investigation under the *Whistle-blower's Act* and conduct, supervise, or coordinate such inquiries, investigations, or reviews as appropriate.
- Report expeditiously to the Department of Law Enforcement or other law enforcement agencies, as appropriate, whenever the inspector general has reasonable grounds to believe there has been a violation of criminal law.
- Conduct investigations and other inquiries free of actual or perceived impairment to the independence of the inspector general or the OIG. This shall include freedom from any interference with investigations and timely access to records and other sources of information.

Complaints and Requests for Assistance

The Investigations Section processed 74 new complaints or requests for assistance. The complaints or requests for assistance were received from current and former state agency employees, independent contractors, the public, other state agencies, the Office of the Chief Inspector General, or anonymous sources.

The complaints or requests for assistance were received by mail, telephone, email message, or in person. The complaints or requests for assistance were generally categorized as:

- Violations of Department policy;
- Employee or contractors of the Department, Florida Commission on Human Relations (FCHR), or Florida Department of Corrections (FDC);
- Member service staff of the Florida Retirement System or People First System;
- Defrauding of the Florida Retirement System;
- Health and safety or policy violations within FDC correctional institutions or the private correctional facilities;¹ and
- Outside of the OIG jurisdiction, including private businesses, other state agencies, or county and local governments.

Complaints or Requests for Assistance Dispositions

All complaints or requests for assistance were assigned a case number for tracking and follow-up. Additionally, all complaints were assessed to determine if the complainant and the nature of disclosed information met the qualifications stated in the *Whistle-blower’s Act*. The Investigations Section performed detailed determinations on 17 complaints, and none met the provisions of the Whistle-blower’s Act.



Table 2 depicts how the Investigations Section closed 126 complaints or requests for assistance received during the fiscal year which included 67 complaints or requests for assistance from prior fiscal years.

Table 2 – Disposition of Complaints or Requests for Assistance

Count	Disposition
39	Administratively closed with the transfer of the private correctional facilities to FDC.
28	Handled by OIG. Obtained additional information; investigated; had no jurisdiction; or due to lack of information closed the complaint.
27	Referred to Department division management for review and response or action deemed appropriate.

¹ Effective October 1, 2023, Chapter 2023-268, Laws of Florida, transferred from the Department to FDC all powers, duties, functions, records, personnel, associated administrative support positions, property, administrative authority, and administrative rules relating to private correctional facilities by a type two transfer, as defined in § 20.06(2), Florida Statutes. The Department formerly managed contracts for Bay Correctional Facility; Blackwater River Correctional Facility; Gadsden Correctional Facility; Graceville Correctional Facility; Lake City Youthful Offender Facility; Moore Haven Correctional Facility; and South Bay Correctional Facility.

Table 2 – Continued

Count	Disposition
25	Referred to law enforcement for incidents that were potential criminal violations.
4	Referred to other entities, such as state or federal agencies or the Office of the Chief Inspector General, for review and response or action deemed appropriate.
3	Replied to public records requests.
126	Total Complaints or Request for Assistance Closed.

Summary of Investigations Closed

Case Number 2024.19 – Issued: November 2023

The Investigations Section initiated an investigation into allegations that an employee sexually harassed a coworker. The investigation revealed inconsistencies and conflicting testimony by the complainant and witnesses which did **not support** the sexual harassment allegation. However, the information obtained during the investigation **supported** the employee’s conduct was unprofessional and unbecoming of a state employee. During the investigation, it was determined the complainant offered to falsely create a sexual harassment complaint against a coworker and admitted dishonesty under oath. These additional findings were determined to be in violation of Department policies and procedures and were **supported**.

Summary of Preliminary Inquiries Closed

Case Number 2024.59 – Issued: May 2024

The Investigations Section initiated a preliminary inquiry into allegations that two employees used state time and resources in violation of Florida Administrative Code and Department policies and procedures. Based on information obtained during the preliminary inquiry, a law enforcement referral was completed and the complaint was closed.

Accreditation

An accreditation program has long been recognized as a means of maintaining and verifying the highest standards. Accreditation is the certification by an independent reviewing authority that an entity has met specific requirements and prescribed standards. In 2009, the Commission for Florida Law Enforcement Accreditation (CFA) expanded its program to include inspectors general offices.

On October 3, 2018, the full CFA voted unanimously to award the certificate of accreditation to the OIG. The accreditation cycle remains in effect for three years at which point, CFA state assessors complete a re-accreditation review of the OIG.

In October 2021, the full CFA again awarded the OIG a certificate of re-accreditation and the OIG is scheduled for a second re-accreditation review in October 2024.



Internal Audit Activity

Section 20.055, F.S., requires the Inspector General to review and evaluate internal controls necessary to ensure the fiscal accountability of the Department. The Inspector General shall conduct financial, compliance, electronic data processing, and performance audits of the agency and prepare audit reports of the findings.

Internal Audit staff perform independent audits, reviews, and examinations to identify, report and recommend corrective actions for areas of inefficiencies, control deficiencies or non-compliance with applicable laws, rules, policies, and procedures. The internal audit activity helps the Department accomplish its objectives by bringing a systematic, disciplined approach to evaluate and improve the effectiveness of risk management, control, and governance processes.

The Internal Audit Section published six internal audit reports and conducted a follow-up review on 169 corrective actions. The Internal Audit Section also ensured coordination between the Department program areas and external auditors. During the fiscal year, the Department was the subject of three external audits conducted by the Auditor General.

Internal Audit Projects Completed

Internal Audit Report No. 2023-32 – *Enterprise Audit of Identity and Access Management* – Issued: August 1, 2023:

Part 1 – *Health Insurance Management Information System*

Part 2 – *FleetWave*

Part 3 – *Active Directory, Statewide Travel Management System, Budget and Accounting Reporting System*

Part 4 – *Department Policies and Procedures*

The objectives of this audit were to evaluate Department controls and compliance with Rule 60GG-2.003(1), Florida Administrative Code, Identity Management, Authentication, and Access Control, and the requirement that access to information technology resources is limited to authorized users, processes, or devices, and to authorized activities and transactions. The scope of the audit included Department cybersecurity identity management and access control policies, procedures, activities, and process for the selected systems.

This audit is classified as a confidential report pursuant to § 282.318, F.S. and is exempt from the provisions of § 119.07(1), F.S.

Internal Audit Report No. 2023-33 – *Building Automation Systems (BAS)* – Issued: September 29, 2023

The objective of this audit was to evaluate the effectiveness of selected controls related to BAS that ensure the confidentiality, integrity, and availability of the Department network supporting Department systems and applications. The scope of this audit included BAS policies, procedures, activities, processes, systems, and hardware in place during fiscal year 2022-23. BAS include controlling heating, ventilation, and air conditioning (HVAC) equipment and lighting. This audit engagement resulted in 6 findings and 10 recommendations. Management agreed with all reported findings and their responses are included in the report.

This audit is classified as a confidential report pursuant to § 282.318, F.S. and is exempt from the provisions of § 119.07(1), F.S.

Enterprise Audit of Incident Response, Reporting, and Recovery

This was a series that followed the four phases of the National Institute of Standards and Technology (NIST) *Incident Response Life Cycle* and includes an additional phase, *Coordination*, based on requirements of applicable Florida Statutes. The overall objective of this audit was to evaluate Department controls and compliance with incident response, reporting, and recovery requirements contained Rules 60GG-2.001 through 60GG-2.006, F.A.C.

**Report 1: Internal Audit Report No. 2024-25 – *Preparation* –
Issued: January 18, 2024**

This report specifically looked at the life cycle phase *Preparation*. It focused on the establishment of policies and procedures and if those included processes to determine whether an incident occurred, roles and responsibilities for workers and key stakeholders were defined; workers were trained on executing the plan, the plan was tested, and security awareness training was provided for workers.

**Report 2: Internal Audit Report No. 2024-34 – *Detection and Analysis* –
Issued: February 23, 2024**

This report specifically looked at the life cycle phase *Detection and Analysis*. It focused on determining whether the agency had effective cybersecurity incident response capabilities to effectively detect, analyze, and respond to cyber threats.

**Report 3: Internal Audit Report No. 2024-35 – *Containment, Eradication,
and Recovery* – Issued: March 21, 2024**

This report specifically looked at the life cycle phase *Containment, Eradication, and Recovery*. It focused on determining whether the Agency internal controls were functioning effectively to prevent further damage, reduce the immediate impact of the incident, and allow the return to normal operations.

**Report 4: Internal Audit Report No. 2024-35 – *Containment, Eradication,
and Recovery* – Issued: March 21, 2024**

This report specifically, the life-cycle phase *Post-Incident Activity*. It focused on whether internal controls were functioning effectively when documenting incidents, informing Department leadership, hardening the environment to prevent similar incidents, and applying lessons learned to improve the handling of future incidents. Coordination focused on determining if the Department effectively coordinated with the Cybersecurity Operations Center (CSOC) within Florida [Digital Service] and the Florida Department of Law Enforcement (FDLE) throughout the life cycle phase.

These audits are classified as confidential reports pursuant to § 282.318, F.S. and are exempt from the provisions of § 119.07(1), F.S.

External Audit Coordination

Section 20.055, F.S., requires the OIG to ensure effective coordination and cooperation between the Auditor General, federal auditors, and other governmental bodies with a view toward avoiding duplication. The OIG is the primary liaison with external entities and is responsible for coordinating and facilitating responses to audits or reviews by those entities. To meet the statutory requirement, the Internal Audit Section coordinates information requests and management responses between external auditors and management and, as requested, assists with scheduling meetings. When the external audit is complete and the preliminary and tentative findings have been issued, the Internal Audit Section coordinates the required management responses.

During the fiscal year, the Internal Audit Section coordinated three external audits completed by the Auditor General. The completed external audits contained zero recommendations for the Department. Table 3 shown below lists the completed external engagements.

Table 3 – External Audit Coordination Completed

Auditor General Report Number	Audit Subject	Report Date
2024-013	<i>Florida Retirement System Pension Plan and Retiree Health Insurance Subsidy Program Cost-Sharing Multiple Employer Defined Benefit Plans Deferred Outflows for Contributions Subsequent to the June 30, 2022, and June 30, 2021, Measurement Dates by Employer Fiscal Year Ended June 30, 2023, and 2022</i>	September 1, 2022
2024-093	<i>Florida Retirement System Pension Plan and Other State Administered Systems Annual Comprehensive Financial Report Fiscal Year Ended June 30, 2023</i>	December 15, 2023
2024-109	<i>Schedules of Employer Allocations and Pension Amounts by Employer for the Florida Retirement System Pension Plan and the Retiree Health Insurance Subsidy Program Cost-Sharing Multiple Employer Defined Benefit Pension Plans For Fiscal Year Ended June 30, 2023</i>	January 12, 2024

Follow-up Activities

Section 20.055, F.S., the *Standards and Principles and Standards for Offices of Inspector General* require the OIG to establish a follow-up process to monitor and ensure management implemented corrective actions.

During Fiscal Year 2023-2024, the Internal Audit Section performed a review of the status of corrective action taken by the Department in response to reported findings and recommendations. Report No. FP 2024-28, *Status Report on Corrective Action Implementation*, issued July 1, 2024, included 169 corrective actions from 27 prior audit projects and 1 special project. The review noted that 30 corrective actions were administratively transferred to the Department of Corrections and Florida State University. For the remaining 139 corrective

actions, management advised that 42 were ready for review. Our review determined that 34 corrective actions were complete with 6 of them pending confirmation from the Office of the Auditor General (AG); 3 corrective actions were superseded by newer identical or related subsequent findings; and management had not fully implemented corrective actions for 5.

It is Internal Audit Section policy to continue to monitor outstanding findings and recommendations until corrective action has been implemented or management accepts the risk of not implementing the recommendations.

Table 4 shown below lists the 27 prior audits included in the follow-up review.

Table 4 – Follow-up Reviews Completed

No.	Report Number	Audit Subject
1	AG 2021-112	<i>Operational Audit of Department of Management Services (DMS) Selected Administrative Activities and Prior Audit Follow-up</i>
2	AG 2022-179	<i>Information Technology Operational Audit of DMS State Data Center Operations</i>
3	AG 2022-203	<i>Operational Audit of DMS Oversight of Private Correctional Facilities</i>
4	AG 2023-022	<i>Information Technology Operational Audit of DMS Integrated Retirement Information System (IRIS)</i>
5	IA 2017-25	<i>Audit of the Management of Third Party Service Providers</i>
6	IA 2020-36	<i>Audit of Cybersecurity with a Focus on Malware</i>
7	IA 2020-56	<i>Audit of the State Data Center’s Disaster Recovery Service</i>
8	IA 2020-57	<i>Audit of the Department’s Revenue and Accounts Receivable Processes</i>
9	IA 2020-65	<i>Audit of State Data Center’s Use of the State Term Contract for Information Technology Staff Augmentation Services</i>
10	IA 2020-69	<i>Information Technology Audit of Remote Desktop Protocol</i>
11	IA 2021-39	<i>Audit of the Office of Supplier Diversity</i>
12	IA 2021-85	<i>Audit of Communications Service Authorization Billing (CASB) System</i>
13	IA 2022-24	<i>Audit of Information Technology Governance</i>
14	IA 2022-27	<i>Enterprise Audit of Cybersecurity Continuous Monitoring</i>
15	IA 2022-28	<i>Audit of Accounts Payable</i>
16	IA 2022-29	<i>Audit of Departmental Purchasing</i>
17	IA 2022-35	<i>Active Directory</i>
18	SP 2023-21	<i>Performance Measure Review (Office of Supplier Diversity)</i>
19	IA 2023-32-1	<i>Enterprise Audit of Identity and Access Management Part 1 of 4 – Health Insurance Management Information System (HIMIS)</i>
20	IA 2023-32-2	<i>Enterprise Audit of Identity and Access Management Part 2 of 4 – FleetWave</i>
21	IA 2023-32-3	<i>Enterprise Audit of Identity and Access Management Part 3 of 4 – Active Directory, Statewide Travel Management System (STMS), and Budget and Accounting Reporting System (BARS)</i>
22	IA 2023-32-4	<i>Enterprise Audit of Identity and Access Management Part 4 of 4 – Department Policies and Processes</i>
23	IA 2023-33	<i>Building Automation Systems</i>

Table 4 – Continued

No.	Report Number	Audit Subject
24	IA 2024-25	<i>Enterprise Audit of Incident Response, Reporting, and Recovery (EIRRR) – Preparation</i>
25	IA 2024-34	<i>EIRRR – Detection and Analysis</i>
26	IA 2024-35	<i>EIRRR – Containment, Eradication, and Recovery</i>
27	IA 2024-36	<i>EIRRR – Post-Incident Activity and Coordination</i>

Significant Outstanding Recommendations from Prior Annual Reports

Section 20.055, F.S., requires the identification of each significant recommendation described in previous annual reports on which corrective action has not yet been completed. The significant outstanding recommendations from prior annual reports are detailed in **Appendix A: Outstanding Recommendations** of this report.

Oversight Activities

The OIG has numerous activities that are classified as oversight. These include OIG risk assessments, OIG work plans, OIG annual reports, internal/external assistance activities, OIG quality assurance and improvement program, and outreach and education activities. During the fiscal year, the OIG performed the following oversight activities.

OIG Risk Assessment, Annual Work Plan, and Annual Report

In accordance with § 20.055, F.S., the OIG develops long-term and annual work plans, based on the findings of a comprehensive annual risk assessment. The annual work plan is approved by the Department secretary and submitted to the chief inspector general and the Auditor General. The OIG is also responsible for preparing an annual report summarizing the activities of the office during the immediately preceding fiscal year.

Internal Audit Section Risk Assessment and Plan for Fiscal Year 2023-2024

The Internal Audit Section’s annual work plan is based on the results of the annual risk assessment. The annual risk assessment process includes interviewing executive management and surveying Department division directors and managers to identify areas of risk to the Department and areas of concern for management. The risks are analyzed and ranked to determine the highest risks and priority for audit and review. The purpose of developing the annual work plan is to identify, select, and plan the allocation of resources for the upcoming fiscal year. The Internal Audit Section’s goal is to provide, as efficiently as possible, the greatest level of assurance and consulting services to the Department.

Internal/External Assistance Activities

Cybersecurity Incident Response Team (CSIRT)

The CSIRT responds to suspected cybersecurity incidents by identifying and controlling incidents, notifying designated CSIRT responders, and reporting findings to Department

management. During the fiscal year, the OIG assisted on CSIRT events and provided input into policies and procedures for the CSIRT.

Legislative Budget Request

The OIG prepared *Schedule IX: Major Audit Findings and Recommendations (Schedule IX)* for the Legislative Budget Request of the Department. The *Schedule IX* is designed to inform decision makers on recent major findings and recommendations found in Auditor General and OIG reports issued during the current and previous fiscal years. The *Schedule IX* also provides information on the status of action taken to correct reported deficiencies and is cross-referenced to any budget issues for funding needed to implement audit recommendations.

Florida Single Audit Act Activities

The OIG reviews submissions for new Catalog of State Financial Assistance (CSFA) numbers to the Department of Financial Services. Additionally, the OIG assists management and external parties regarding the Florida Single Audit Act processes and requirements.

Executive Order 20-44

In February 2020, Governor DeSantis issued Executive Order 20-44 regarding sole-source, public-private agreements and other specific contracts and agreements. As part of the instructions, agencies must submit an attestation form to their Office of Inspector General each year by May 31. The OIG coordinated with Department management to ensure timely submission of the attestation.

OIG Quality Assurance and Improvement Program

The OIG is statutorily required to follow the *Standards*. Standard 1300 requires that the chief audit executive develop and maintain a quality assurance and improvement program (QAIP) that covers all aspects of the internal audit activity. The QAIP consists of both an internal quality assurance program, that is ongoing and includes continuous supervision and periodic self-assessments; and external quality assessments conducted by the Auditor General every three years in accordance with § 11.45, F.S.

Enterprise Projects

To gain efficiency of working together, the Chief Inspector General and agency inspectors general meet on a regular basis to discuss and evaluate enterprise issues and projects. Additionally, the OIG assists staff from various OIGs with special requests and provides support for Enterprise projects.

During Fiscal Year 2023-2024, the OIG participated in American Rescue Plan Act Agency Coordinated Response calls. The OIG also participated in conducting the Enterprise Risk Assessment with the Office of the Chief Inspector General to determine the next audit topic for the enterprise cybersecurity audit.

Cybersecurity Training

Based on efforts of the Chief Inspector General and funding from the Florida Legislature the OIG was able to participate in multiple Cybersecurity webinars and trainings this past fiscal

year. These trainings enabled members of the OIG to gain greater cybersecurity knowledge and skills. Topics included: Insider Threats; Cybersecurity Fundamentals; Incident Response, Recovery, and Reporting; Risk Management Framework; Introduction to Cyber Investigations; Malware Incident Response and Investigation; and Handling, Investigating, and Responding to Email Incidents.

Outreach and Education Activities

New Employee Orientation

During Department new employee orientation sessions, the OIG presents an overview of the roles and responsibilities of the OIG. This presentation is designed to provide new employees with a basic understanding of the OIG and how each employee plays an important role in the identification and prevention of fraud, waste, and abuse within the Department. The presentation also includes an explanation of the Florida Whistle-blower's Act and how it applies to Department employees.

During the new employee orientation sessions, each new employee is provided an OIG brochure which details the pertinent Department policies and procedures related to the OIG and includes contact information on how to reach the OIG.

Fraud Awareness

The OIG presents fraud deterrence information to internal and external audiences in an effort to identify or prevent significant violations of governing directives. During the fiscal year, the OIG updated its internal website and OIG brochures for distribution to Department employees in order to raise awareness of OIG duties, responsibilities, and how employees can help the OIG to identify fraudulent activity.

Cybersecurity Incident Response Team (CSIRT) Training Exercises

Members of the OIG staff participated as non-technical observers for the annual Florida Digital Service CSIRT training exercises were conducted in October. The OIG staff provided feedback to Florida Digital Service on CSIRT soft skills, such as team engagement, communication, coordination, compliance with their policy and procedures, and teamwork.

Appendix A: Outstanding Recommendations

Section 20.055, F.S., requires the identification of each significant recommendation described in previous annual reports on which corrective action has not yet been completed. The significant outstanding recommendations from prior annual reports are detailed below.

Internal Audit Report No. 2017-25: *Management of Third-Party Service Providers* Issued: December 29, 2017

The purpose of this audit was to provide management with assurances that divisions within the Department had adequate and effective procedures and controls for managing service providers and that the procedures and controls in place to manage service providers included recognized best practices and complied with applicable statutes, rules, regulations, policies, and procedures.

The audit included the following recommendations where corrective action has not yet been completed:

- We recommended that management update policies and procedures regarding monitoring service providers to include specific procedures for performing risk assessments as a part of developing a monitoring plan. In addition, we recommended that these procedures include the criteria and evaluation method for conducting risk assessments as well as requirements regarding the frequency of risk assessments. Including this information in the Department policies and procedures will help ensure consistency and more effective monitoring of service providers' performance. Also, it will help ensure compliance with the Florida Certified Contract Manager (FCCM) Participant Guide.
- We recommended that management update policies and procedures related to contract monitoring to include specific guidance and requirements for the following:
 - Preparing a monitoring plan,
 - Frequency of plan update,
 - Documentation and evidence of monitoring activities to be obtained and maintained, and
 - Procedures for independently validating and verifying service provider deliverables (i.e., reports and data) and performance.

Management should take steps to ensure that updated policies and procedures include Department minimum expectations as well as all requirements outlined in Chief Financial Officer (CFO) Memorandum #6 (11-12). Also, we recommended that management provide internal training to division staff to ensure that expectations and requirements are clear.

- We recommended that management update policies and procedures related to payment processing to include specific requirements for timely invoice processing, compliance with related statutes regarding contract manager certification and compliance with rules regarding contract manager delegation. Also, we recommended that management provide internal training to division staff to ensure that expectations and requirements are clear regarding prompt payment, interest penalties, contract manager certification, and delegation of responsibilities.

- We recommended that management update policies and procedures related to contract monitoring to include specific requirements for developing corrective action plans and performing follow-up to such plans. Management should take steps to ensure that the update includes minimum expectations of the Department. Also, we recommended that management provide internal training to division staff to ensure that expectations and requirements are clear. Finally, we recommended that management consider updating the contract templates to include procedures for ensuring corrective action and follow-up to any required corrective actions.
- We recommended that management update policies and procedures related to contract management and monitoring to include all components for closing out a contract as documented in the FCCM Participant Guide. Management should take steps to ensure that this update includes Department minimum expectations for closing out contracts. The policies and procedures should ensure that all contract terms and conditions are met and all outstanding issues have been resolved prior to final payment to the service providers. Also, the procedures should ensure the official contract files contain all necessary closeout documentation. Finally, we recommended that management provide internal training to division staff to ensure that expectations and requirements are clear.
- We recommended that management consider implementing procedures to separate some of the duties performed by the contract manager or implementing additional control procedures to compensate for areas with limited segregation of duties.
- We recommended that Departmental Purchasing management implement procedures to ensure that contract file review is completed and to ensure the timely correction of any discrepancies.

Internal Audit Report No. 2020-57: *Audit of The Department's Revenue and Accounts Receivable Processes*
Issued: December 30, 2020

The purpose of this audit was to determine if the Department maintained an effective system of internal controls over revenue and accounts receivable.

The audit included the following recommendations where corrective action has not yet been completed:

- We recommended that the Financial Management Services (FMS) Bureau Chief:
 - Update the Accounts Receivables Policy to include a review process that will ensure accounts receivable are referred to a Department of Financial Services-contracted collection agent before accounts are 120 days past due.
 - Perform a review, no less than quarterly, of accounts receivable aging reports to ensure that all delinquent accounts receivable have been referred to a collection agent.

Internal Audit Report No. 2020-65 – *Audit of State Data Center’s Use of State Term Contract for Information Technology Staff Augmentation Services*
Issued: November 6, 2020

The purpose of this audit was to determine if the State Data Center (SDC) followed the purchasing procedures and implemented oversight and management controls related to the use of the *State Term Contract for Information Technology Staff Augmentation*.

The audit included the following recommendations where corrective action has not yet been completed:

- We recommended the Departmental Purchasing Director create guidance specific to contract management of purchases from a state term contract including necessary items that should be maintained in the contract file.
- We recommended that the Departmental Purchasing Director update Purchasing 101 and include the current purchasing standards, laws, and rules.

Internal Audit Report No. 2020-69 – *Information Technology Audit of Remote Desktop Protocol*
Issued: April 27, 2021

The objective of the audit was to review the information technology security controls related to accessing non-public computing resources by a remote workforce. This audit is classified as a confidential report pursuant to § 282.318, F.S. and is exempt from the provisions of § 119.07(1), F.S.

Internal Audit Report No. 2021-39 – *Audit of Office of Supplier Diversity*
Issued: December 11, 2020

The purpose of the audit was to determine if internal controls related to the security of personal and confidential information in the Office of Supplier Diversity (OSD) were adequate and operating effectively.

The audit included the following recommendations where corrective action has not yet been completed:

- The OIG recommended that the Deputy Director of Operations ensures periodic reviews of access privileges are performed and documented for OSD Apps users to ensure that only authorized users have access and that the access privileges provided to each user remain appropriate.

Internal Audit Report No. 2022-24 – *Audit of Information Technology Governance*
Issued: April 26, 2022

The objective of the audit was to assess the degree to which Department information technology (IT) governance activities were consistent with Florida Statutes and Florida Administrative Code. This audit is classified as a confidential report pursuant to § 282.318, F.S. and is exempt from the provisions of § 119.07(1), F.S.

Internal Audit Report No. 2022-27 – Enterprise Audit of Cybersecurity Continuous Monitoring

Issued: July 27, 2022

The objective of the audit was to evaluate Department controls and compliance with Chapter 60GG-2.004(2), F.A.C., *Security Continuous Monitoring* regarding information technology resource monitoring to identify cybersecurity events. This included:

- a) Monitoring the network to detect potential cybersecurity events.
- b) Monitoring the physical environment to detect potential cybersecurity events.
- c) Monitoring user activity to detect potential cybersecurity events.
- d) Monitoring for malicious code.
- e) Monitoring for unauthorized mobile code.
- f) Monitoring for external service provider activity to detect potential cybersecurity events.
- g) Monitoring for unauthorized personnel, connections, devices, and software.
- h) Performing vulnerability scans which are part of the System Development Life Cycle.

This audit is classified as a confidential report pursuant to § 282.318, F.S. and is exempt from the provisions of § 119.07(1), F.S.

Internal Audit Report No. 2022-29 – Audit of Departmental Purchasing

Issued: May 13, 2022

The purpose of the audit was to perform a risk-based compliance audit to determine if the Bureau of Departmental Purchasing complies with laws, rules, regulations, policies, and procedures, and evaluate any trends in vendor preference. This audit satisfied the requirements of House Bill 1079, passed during the 2021 Legislative Session, which amended § 287.136, F.S., to require a periodic risk-based compliance audit of all contracts executed by a state agency to identify any trends in vendor preferences.

The audit included the following recommendations where corrective action has not yet been completed:

- We recommended Departmental Purchasing and Real Estate Development and Management ensure contract information and documents are entered into FACTS within 30 days of contract execution as required by § 215.985(14)(a), F.S.

Internal Audit Report No. 2022-35 – Active Directory

Issued March 6, 2023

The objective of the audit was to evaluate the effectiveness of managerial and technical controls of the Department Active Directory System. This audit is classified as a confidential report pursuant to § 282.318, F.S. and is exempt from the provisions of § 119.07(1), F.S.

**Auditor General Report No. 2021-112 – Department of Management Services
Selected Administrative Activities and Prior Audit Follow-up
Issued: January 21, 2021**

This operational audit of the Department focused on selected administrative activities and included a follow-up on applicable findings noted in Auditor General (AG) report Nos. 2019-098 and 2017-214.

The audit included the following AG recommendations where corrective action has not yet been completed:

- The AG recommended that Department management establish policies and procedures for administering the requirements of the Florida Single Audit Act, including policies and procedures for identifying non-State entities required to submit a Financial Reporting Package (FRP), tracking the receipt and review of FRPs, and determining whether timely and appropriate corrective action was taken for applicable audit findings and recommendations.
- The AG also recommended that Department management strengthen controls to ensure that State Financial Assistance is appropriately recorded in Department records. We recommended that Department management restrict user access privileges to FLAIR to promote an appropriate separation of duties and require that, where incompatible access privileges are necessary, compensating controls are established and documented. Department management should also ensure that FLAIR access privileges are removed immediately upon an employee's separation from Department employment.
- The AG recommended that Department management enhance policies and procedures to ensure that all personnel responsible for managing contracts are subject to Department conflict of interest policies and procedures and that all contract managers complete conflict of interest statements evidencing that they are independent of, and have no conflicts of interest related to, the contracts they are responsible for managing.

**Auditor General Report No. 2022-179 – Information Technology Operations Audit
of the Department of Management Services, State Data Center Operations
Issued: March 28, 2022**

This operational audit of the Department focused on evaluating selected IT controls applicable to State Data Center (SDC) operations. The audit also included a follow-up on the findings included in AG report No. 2020-149.

The audit included the following recommendations where corrective action has not yet been completed:

- The AG again recommended that Department management improve certain security controls related to logical access, vulnerability management, configuration management, user authentication, and logging and monitoring to ensure the confidentiality, integrity, and availability of SDC and customer entity data and related IT resources.

**Auditor General Report No. 2022-022 – Department of Management Services
Information Technology Operational Audit of the Integrated Retirement
Information System (IRIS)
Issued: August 17, 2022**

This operational audit focused on evaluating selected IRIS information technology controls and included a follow-up on applicable findings included in AG report number 2019-220.

The audit included the following recommendations where corrective action has not yet been completed:

- The AG recommended that division management improve IRIS change management controls to ensure that all program changes are appropriately authorized, tested, reviewed, and approved prior to implementation into the production environment, and are managed by, and do not bypass, the divisions change management process.
- The AG recommended that Department and division management improve certain security controls related to logical access, user authentication, configuration management, and logging and monitoring to ensure the confidentiality, integrity, and availability of IRIS data and related IT resources.

DMS

