

Executive Office of the Governor

OFFICE OF THE CHIEF INSPECTOR GENERAL

**2025 - 2026
ANNUAL REPORT**

**Presented
September 30, 2026**



**The Honorable Ron DeSantis
Governor of Florida**

**Melinda M. Miguel
Chief Inspector General**



RON DESANTIS
GOVERNOR

STATE OF FLORIDA
Office of the Governor

THE CAPITOL
TALLAHASSEE, FLORIDA 32399-0001

www.flgov.com
850-717-9418

September 30, 2026

The Honorable Ron DeSantis
Governor of the State of Florida
The Capitol, PL 05
Tallahassee, Florida 32399-0001

Dear Governor DeSantis:

In accordance with section 20.055, Florida Statutes, I am pleased to submit the Office of the Chief Inspector General's Annual Report for fiscal year 2025-2026. This report highlights our efforts and activities during the preceding fiscal year.

As this report demonstrates, the Office of the Chief Inspector General is committed to providing leadership in the promotion of accountability, integrity, and public trust in government.

Respectfully,

A handwritten signature in blue ink, reading "Melinda M. Miguel".

Melinda M. Miguel
Chief Inspector General



Executive Office of the Governor
Office of the Chief Inspector General
Annual Report FY 2025-2026

Office of the
CHIEF INSPECTOR GENERAL

TABLE OF CONTENTS

EXECUTIVE SUMMARY	1
INTRODUCTION	4
INDEPENDENCE	4
PROFESSIONAL STANDARDS AND CODE OF ETHICS	5
STRATEGIC PLAN METRICS	5
ORGANIZATION AND STAFFING.....	7
CHIEF INSPECTOR GENERAL PROJECTS OR ACTIVITIES.....	9
INVESTIGATIVE ACTIVITY	26
AUDIT ACTIVITY.....	31
FINANCIAL EMERGENCY ACTIVITY	35
CONCLUSION.....	37



Executive Office of the Governor
Office of the Chief Inspector General
Annual Report FY 2025-2026

EXECUTIVE SUMMARY



In accordance with § 14.32, Florida Statutes (F.S.), and § 20.055, F.S., the Office of the Chief Inspector General is responsible for promoting accountability, integrity, and efficiency in the Executive Office of the Governor and in agencies under the jurisdiction of the Governor.

Consistent with these responsibilities, the Office of the Chief Inspector General completed the following activities during Fiscal Year (FY) 2025-2026:

- Received, reviewed, and processed 4,651 complaints and requests for assistance by Florida's citizens and government employees and closed 4,608 such complaints and requests;
- Received, reviewed, and processed 4,203 pieces of additional information from Florida's citizens and government employees for existing correspondences;
- Completed, reviewed, or processed 195 whistle-blower determinations prepared by Inspectors General in accordance with the provisions of §§ 112.3187 - 112.31895, F.S. (Florida's Whistle-blower's Act). Of those determinations, 13 met the statutory provisions to be designated as a whistle-blower complaint;
- Provided oversight for 15 whistle-blower investigations. Seven (7) of those, conducted by agency Inspectors General and State Universities, were closed during FY 2025-2026. Of the seven (7), the Office of the Chief Inspector General reviewed and issued three (3) final reports to mandatory recipients in compliance with § 112.3189(9)(c), F.S.;
- Completed or assisted with eight (8) non-whistle-blower investigations, reviews, inspections, or audits;
- Participated in two (2) Florida Digital Service (FLDS) workgroups, one (1) Council (the Florida Cybersecurity Advisory Council),¹ and three (3) Florida Cybersecurity Advisory Council workgroups;

¹ The Cybersecurity Advisory Council is established in § 282.319, Florida Statutes (F.S.), to assist state agencies in protecting their information technology resources from cyber threats and incidents. The Chief Inspector General is a designated voting member of the Council. However, internal policies provide for the Chief Inspector General to be advisory in nature, not in an operational capacity, to preserve independence according to professional standards.



**Executive Office of the Governor
Office of the Chief Inspector General
Annual Report FY 2025-2026**

- Trained a total of 309 state and local personnel through 19 training sessions provided through the Office of the Chief Inspector General's Cyber Pathways Program;
- Received and processed 192 final audit reports and corrective actions, pursuant to § 20.055(6)(f) and (h), F.S., which require Inspectors General in agencies under the jurisdiction of the Governor to submit final audit reports and provide information related to significant findings and related corrective action plans to the Chief Inspector General;
- Received 23 FY 2025-2026 annual audit plans by Inspectors General pursuant to § 20.055(6)(i), F.S., which requires Inspectors General to develop long-term and annual audit plans based on the findings of periodic risk assessments. In agencies under the jurisdiction of the Governor, Inspectors General are required to submit their annual audit plans, and any revised annual audit plans, to the Chief Inspector General;²
- Received, reviewed, and processed 61 notifications and consultations pursuant to § 20.055(2)(f), F.S., which requires Inspectors General in agencies under the jurisdiction of the Governor to keep the Chief Inspector General informed concerning fraud, abuses, and deficiencies related to programs and operations administered or financed by the state agency; recommend corrective action(s) concerning fraud, abuses, and deficiencies; and report on the progress made in implementing corrective action(s);
- Reviewed 140 personnel actions pursuant to § 20.055(3)(b), F.S., which requires Inspectors General in agencies under the jurisdiction of the Governor to hire or remove personnel in consultation with the Chief Inspector General but independently of their agency;
- Served as the Governor's designee for financial emergencies pursuant to § 218.503, F.S.;
- Contacted 30 local governmental entities to gather information for use in determining financial emergency status in accordance with § 218.503, F.S.;
- Provided technical assistance in accordance with Executive Order Number 16-135 to resolve the state of financial emergency of the City of Opa-Locka, worked with the financial emergency board, and served as the lead "agency" to carry out the Executive Order and agreement with the City;

² Pursuant to § 20.055(6)(i), F.S., audit plans are also submitted to the agency head for approval and the approved audit plan is submitted to the Auditor General.



**Executive Office of the Governor
Office of the Chief Inspector General
Annual Report FY 2025-2026**

- Coordinated and conducted 18 case management conferences³ with Offices of Inspector General in agencies under the jurisdiction of the Governor;
- Delivered statewide capability-building through the Cyber Pathways Program, equipping Inspector General staff with training, tools, and audit support to strengthen Florida's enterprise cybersecurity oversight and ensure agencies are prepared to assess and validate cybersecurity practices;
- Facilitated collaboration between the Executive Office of the Governor, the Auditor General, federal auditors, and other governmental entities to prevent redundancy and duplication in their external audit requests; and
- Conducted a nationwide search to identify qualified candidates for the vacant Inspector General position within the Department of Citrus, resulting in the appointment of an Inspector General for this agency.

This report presents detailed information about these accomplishments.

³ Case management conferences are established to maximize the flow of information between state agency Offices of Inspector General and the Office of the Chief Inspector General to ensure the requirements of § 20.055(2)(j), F.S., and compliance with the *General Principles and Standards for Offices of Inspector General*, as published by the Association of Inspectors General, are met.



**Executive Office of the Governor
Office of the Chief Inspector General
Annual Report FY 2025-2026**

INTRODUCTION



The Chief Inspector General has a broad range of responsibilities outlined in § 14.32, F.S., and § 20.055, F.S. These responsibilities include: carrying out activities designed to deter, detect, prevent, and eradicate fraud, waste, abuse, mismanagement, and misconduct in government; initiating, supervising, and coordinating investigations; coordinating complaint-handling activities with agencies; coordinating activities of Florida's Whistle-blower's Act and maintaining the Whistle-blower's Hotline; conducting, directing, and supervising audit activities; monitoring activities of agency Inspectors General; issuing and serving subpoenas; and conducting special investigations and management reviews at the request of the Governor. The Chief Inspector General is also responsible for appointing and removing Inspectors General in agencies under the jurisdiction of the Governor. In addition, when a local governmental entity meets statutory conditions specified in § 218.503(1), F.S., the Governor has delegated responsibilities described within §§ 218.50 - 218.504, F.S., Local Governmental Entity and District School Board Financial Emergencies, to the Chief Inspector General.

Our mission is to assist the Executive Office of the Governor in the accomplishment of its objectives by conducting, supervising, and coordinating accountability activities to enhance public trust in government. During the past year, the Office of the Chief Inspector General worked diligently to meet statutory mandates and ensure standards of excellence were applied consistently across state agencies by agency Inspectors General.

The details of the activities performed by the Office of the Chief Inspector General during FY 2025-2026 related to our responsibilities and mission are detailed below.

INDEPENDENCE

According to § 14.32(4), F.S., and § 20.055(3), F.S., the Chief Inspector General serves as the Inspector General for the Executive Office of the Governor and reports directly to the Governor to ensure audits, investigations, and other activities are performed with competence and independence, and ensure findings and conclusions are developed in accordance with applicable professional standards. Additionally, by statute, the Chief Inspector General is not subject to supervision by any other employee except the Governor and the agency head or staff shall not prevent or prohibit the Chief Inspector General from initiating, carrying out, or completing any audit or investigation.



Executive Office of the Governor
Office of the Chief Inspector General
Annual Report FY 2025-2026

PROFESSIONAL STANDARDS AND CODE OF ETHICS

Pursuant to § 20.055(2)(j), F.S., the Office of the Chief Inspector General complies with the *Principles and Standards for Offices of Inspector General*, as published and revised by the Association of Inspectors General. Staff members abide by the Florida Code of Ethics for Public Officers and Employees, as codified in §§ 112.311 - 112.326, F.S., and the Executive Office of the Governor's Code of Ethics. Internal audits are conducted in accordance with the *Global Internal Audit Standards*, published by the Institute of Internal Auditors, Inc. (IIA).

STRATEGIC PLAN METRICS

The *Global Internal Audit Standards*, Domain IV, Principle Nine, *Plan Strategically*, requires the Chief Audit Executive to plan strategically to position the internal audit function to fulfill its mandate and achieve long-term success. Strategic planning requires that the Office of the Chief Inspector General develop a strategy to comprehend the governance, risk management, and control processes of the Executive Office of the Governor and support its effective operation.

After performing a detailed Strengths, Weaknesses, Opportunities, and Threats (SWOT) analysis and consultation with Executive Office of the Governor senior management, including a review of the priorities of Governor DeSantis,⁴ a Strategic Plan (Plan) was developed for the Office of the Chief Inspector General. The Plan provides the vision, objectives, and strategies for the Office of the Chief Inspector General. This Plan is designed to help us achieve our vision to be a preeminent organization, promote positive change and continuous improvement, and foster an environment of accountability, oversight, and innovation that inspires trust and confidence in our work.

The Plan includes the following four strategic goals for the Office of the Chief Inspector General:

- Goal 1: Oversight – Provide effective and meaningful oversight of the Executive Office of the Governor through audits, investigations, and evaluations to assure the integrity, efficiency, timeliness, and effectiveness of Executive Office of the Governor services and activities.
- Goal 2: Effective Engagement with Stakeholders – Increase mission impact through effective engagement with stakeholders.
- Goal 3: Professional Development and Talent Management – Enhance the performance of both the Office of the Chief Inspector General and state agency

⁴ Please see the Priorities of Governor DeSantis as set forth in the Long-Range Program Plan Instructions provided by the Office of Policy and Budget.



**Executive Office of the Governor
Office of the Chief Inspector General
Annual Report FY 2025-2026**

Offices of Inspector General through strategic investments in employees and resources.

- Goal 4: Innovation – Develop and deploy innovative tools, techniques, and information technology solutions to strengthen the Office of the Chief Inspector General's mission accomplishment and strategically manage organizational growth.

The Office of the Chief Inspector General instituted a process to measure performance with respect to these metrics as noted below:

Oversight:

- We produced six (6) significant written projects and reports (internal audits, internal audit plan, investigations, etc.) to stakeholders within established timeframes.
- We covered 100 percent of all engagement objectives expected to be reviewed in accordance with the internal audit plan.
- We completed 29 consultations, complaint discussions, reporting consultations, investigative report reviews, and whistle-blower determination consultations.
- We issued internal audit reports containing four (4) recommendations for corrective actions to Executive Office of the Governor management.

Effective Engagement with Stakeholders:

- Our stakeholder satisfaction surveys of internal audit clients for completed audit engagement yielded scores of "5.0" on a scale of "1.0" to "5.0," with a score of "5.0" being the highest rating.
- We conducted ethics training sessions with internal staff.
- We developed and delivered 19 separate training sessions to 309 state and local personnel to promote awareness of cybersecurity tools to detect fraud and manage internal controls, risk management, and compliance through our Cyber Pathways Program.

Professional Development and Talent Management:

- We developed, updated, and completed training and development plans for internal staff throughout the fiscal year.
- We instituted recruiting initiatives that leveraged multiple forms of outreach and communication to enhance both our workforce and the workforce of state agency Offices of Inspector General. This includes job postings with relevant professional organizations, such as the National Association of Inspectors General, the Florida Chapter of the Association of Inspectors General, the AGA (formerly known as Association of Government Accountants), and the IIA.



Executive Office of the Governor
Office of the Chief Inspector General
Annual Report FY 2025-2026

- We encouraged staff to participate in professional certification programs, conferences, and industry forums. A listing of all staff professional certifications is included below.
- We established succession planning initiatives to ensure continuity and sustainability of the Inspector General function, including mentoring initiatives both within the Office of the Chief Inspector General and the larger Inspector General community.

Innovation:

- We demonstrated increased capabilities and outcomes from the deployment of innovative information technology. The Office of the Chief Inspector General devoted significant staff time (500 hours in FY 2025-2026) to the integration of Artificial Intelligence (AI) into our audit processes. In accordance with *Global Internal Audit Standard 10.3, Technological Resources*, auditors are required to proactively take steps to enhance the use of technology and develop and broaden their skill sets. Both the Office of the Chief Inspector General's internal audit and investigative staff led a workgroup of state agency Inspectors General, Directors of Auditing, and Chiefs of Investigation to map both internal audit and investigative processes. This effort aimed to identify areas where AI may add value and innovate audit and investigative processes by safely integrating technology, including AI, into all operations.
- We promoted the secure and effective use of data and technology for both staff within the Office of the Chief Inspector General and vendors working under our authority. As an example, we recently strengthened our internal controls for the appropriate use and protection of confidential and exempt information. We updated Office of the Chief Inspector General Office Procedures, to include *Handling Confidential and Exempt Information*, and all vendors working under the auspices of the Office of the Chief Inspector General were made aware of this procedure.

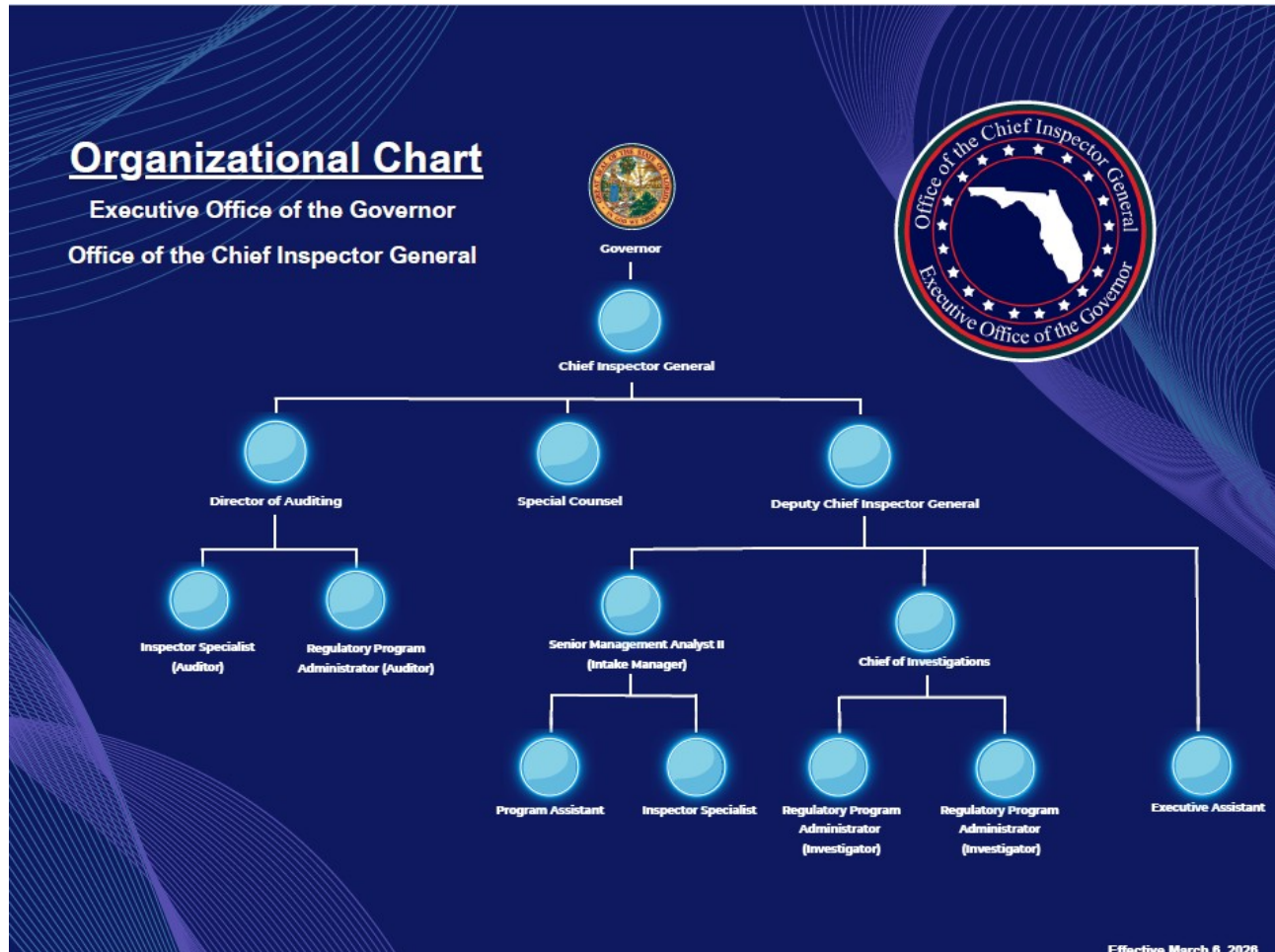
ORGANIZATION AND STAFFING

As of June 30, 2026, the Office of the Chief Inspector General consisted of the following 13 full-time positions: Chief Inspector General, Deputy Chief Inspector General, Director of Auditing, Chief of Investigations, Special Counsel, Senior Management Analyst II, Executive Assistant, two (2) Inspector Specialists, three (3) Regulatory Program Administrators, and a Program Assistant.



Executive Office of the Governor
Office of the Chief Inspector General
Annual Report FY 2025-2026

Office Organizational Chart



Professional Certifications

Members of the Office of the Chief Inspector General hold the following professional certifications:

- Certified Accreditation Manager (1)
- Certified Accreditation Assessor (3)
- Certified Business Manager (1)
- Certified Economic Crime Forensic Examiner (1)
- Certified Construction Auditor (1)
- Certified Cybercrimes Investigator (1)
- Certified Financial Crimes Investigator (1)
- Certified Financial Services Auditor (1)
- Certified Fraud Examiner (1)



Executive Office of the Governor Office of the Chief Inspector General Annual Report FY 2025-2026

- Certified Government Auditing Professional (1)
- Certified Inspector General (2)
- Certified Inspector General Auditor (2)
- Certified Inspector General Counsel (1)
- Certified Inspector General Investigator (2)
- Certified Internal Controls Auditor (2)
- Certified Project Manager (1)
- Construction Control Professional (1)
- Florida Certified Contract Manager (6)
- Notary Public (8)

Professional Organization Affiliations

Office staff maintain affiliations with the following organizations:

- Association of Certified Fraud Examiners (ACFE) (2)
- Association of Government Accountants (AGA) (1)
- Cybersecurity Task Force/Advisory Council (1)
- Florida Bar (2)
- Florida Chapter of the Association of Inspectors General (8)
- Florida Fusion Center (1)
- Information Systems Audit and Control Association (ISACA) (3)
- International Association of Financial Crimes Investigators (1)
- National Association of Inspectors General (5)
- Institute of Internal Auditors, Inc. (4)





Executive Office of the Governor
Office of the Chief Inspector General
Annual Report FY 2025-2026

CHIEF INSPECTOR GENERAL PROJECTS OR ACTIVITIES

During FY 2025-2026, the Office of the Chief Inspector General participated in the following projects or activities:

Monitoring of Legislation

The Office of the Chief Inspector General monitors compliance-related legislation that falls within the scope of its oversight, audit, and investigative authority. This process enables the Office to identify potential impacts on its functions and inform related efforts. This process further allows the Office of the Chief Inspector General to identify potential risks and revise policies to ensure compliance with our statutory oversight responsibilities. In addition, we also monitor legislation and provide analysis at the request of the Office of Policy and Budget within the Executive Office of the Governor.

Legislative Budget Requests

In Fall 2025, the Office of the Chief Inspector General submitted two (2) legislative budget request items for inclusion in the larger Executive Office of the Governor Legislative Budget Request submissions. The Governor included these items in the FY 2025-2026 *Floridians First* budget recommendations.

- \$907,115 in nonrecurring General Revenue for the implementation of a Statewide Procurement and Other Transaction Anomaly Detector. This will provide state agency Offices of Inspector General with a proactive tool to examine financial data and identify anomalous transactions that are not in compliance with programmed business rules, and potentially recoup funds related to fraud, waste, and abuse. The primary goal of this initiative is to ensure integrity in procurement and purchasing processes across state agencies. The tool will identify missing, inconsistent, or duplicate records and illuminate potential indicators of improper payments, fraud, waste, and abuse and other noncompliant transactions. The tool will also flag outlier vendor behavior and uncover potential indicia of fraud.
- \$692,885 in nonrecurring General Revenue to upgrade the Customer Relationship Management (CRM) system. This project will modernize CRM to develop a secure storage solution for sensitive investigative and whistle-blower data to enhance data security, streamline workflows, and implement robust access control mechanisms based on the principles of least privilege and role-based access.



**Executive Office of the Governor
Office of the Chief Inspector General
Annual Report FY 2025-2026**

The Legislature funded both requests and these elements were approved by Governor DeSantis as part of the FY 2026-2027 approved budget.⁵

Compliance Activities for § 287.136(2), F.S.

House Bill 1079, passed in the 2021 Legislative Session and codified in Chapter 2021-225 of the Laws of Florida, included a revision of § 287.136, F.S., that required each agency Inspector General to “complete a risk-based compliance audit of all contracts executed by the agency for the preceding three years” and include in the audit an “evaluation of . . . vendor preference.”

The Office of the Chief Inspector General led the project across the enterprise and was one of 26 participating state agencies in the enterprise engagement completed in FY 2024-2025. The objectives of the engagement were to evaluate all contracts for compliance with Chapter 287, F.S., and other applicable procurement statutes; analyze the overall contract process to identify any trends in vendor preference; and, if applicable, assess the status of corrective actions taken by each agency to address the findings and recommendations included in prior triennial contract audit reports.

The Office of the Chief Inspector General released a roll-up report detailing enterprise findings and recommendations on August 28, 2025. This roll-up report summarizing the results of individual state agency audits collectively indicated that state agencies are generally adhering to fair and open competition principles and are not exhibiting trends in vendor preference. However, systemic weaknesses persisted in areas related to documentation, internal controls, and staff adherence to established procedures and statutory requirements.

The summary report noted that state agencies identified issues with Florida Accountability Contract Tracking System (FACTS) data entry, conflict of interest forms, and record-keeping, which suggested a need for more robust, centralized oversight and continuous training programs to ensure full compliance with § 215.985, F.S. (Transparency Florida Act), and other procurement statutes. Agency audit responses indicated a commitment to addressing these identified issues, with corrective action either initiated or slated for completion soon by Division/Department staff.

City of Opa-Locka Financial Emergency Board

In June 2016, the Governor issued Executive Order Number 16-135, declaring the City of Opa-Locka in a state of financial emergency pursuant to § 218.503, F.S. On June 1, 2016, the City of Opa-Locka’s City Commission ratified the City Manager’s prior request of financial emergency determination to the State. The Governor established a Financial

⁵ See Laws of Florida: Chapter 2026-232.



Executive Office of the Governor Office of the Chief Inspector General Annual Report FY 2025-2026

Emergency Board to oversee the activities of the City of Opa-Locka until their financial emergency is resolved and named the Chief Inspector General as the Governor's designee for carrying out the Executive Order.

Enterprise Cybersecurity Audits

Enterprise cybersecurity audits are conducted to objectively assess agency compliance with the Florida Cybersecurity Standards and the National Institute of Standards and Technology (NIST) Cybersecurity Framework (CSF). These audits are risk-based and authorized under § 20.055(6)(i), F.S., requiring a specific cybersecurity audit plan. Given Florida agencies' interconnected data, infrastructure, and vendor relationships, a single vulnerability may impact multiple entities across the enterprise, underscoring the importance of systematic audits to identify weaknesses and ensure statutory compliance.

These audits give agency leaders objective insight into the maturity of their controls, highlight areas that need additional attention or investment, and strengthen statewide risk management. They also reduce duplication of effort, promote uniform expectations, and support coordinated oversight; helping Florida detect issues earlier, protect sensitive information, and maintain resilient government operations that the public can trust.

Data Protection and Security – FY 2025-2026

Pursuant to § 20.055(6)(i), F.S., a specific cybersecurity audit plan is required. The Office of the Chief Inspector General led this effort within the Executive Office of the Governor and across the state agencies opting in to the project. The topic selected for FY 2025-2026 was Data Protection and Security. This was decided upon in consultation with the Department of Management Services and FLDS leadership and considered workgroup documentation to assess risks facing the enterprise.

The purpose of these audits is to evaluate the effectiveness of controls and compliance with respect to Data Protection and Security requirements contained in Chapter 60GG-2, Florida Administrative Code (F.A.C.), specifically Rule 60GG-2.002 and 2.003(4), F.A.C. The scope of these audits included an evaluation of agency cybersecurity policies, procedures, activities, and processes related to information system Data Protection and Security. In addition to compliance, agency controls were evaluated to determine cybersecurity maturity specific to the objectives as specified in the NIST CSF for the Identify: Governance subcategory (ID.GV-1 and ID.GV-3), and the Protect: Data Security subcategory (PR.DS-1 through PR.DS-8). Across the various agencies, the audits focused on four (4) main fieldwork objectives:



**Executive Office of the Governor
Office of the Chief Inspector General
Annual Report FY 2025-2026**

- **Data Governance** – This objective evaluated whether agencies have established, documented, and communicated cybersecurity policies, roles, responsibilities, and legal/regulatory requirements consistent with Rule 60GG-2, F.A.C., and the NIST CSF. Controls were assessed to determine whether governance processes effectively support risk management, compliance, and oversight throughout the information system boundary.
- **Data at Rest** – This objective examined the extent to which records, devices, and stored information are protected through encryption, secure handling procedures, asset management, and capacity safeguards. Testing focused on whether storage practices, sanitization processes, and data-handling procedures align with state cybersecurity requirements to ensure confidentiality, integrity, and availability of information at rest.
- **Data in Transit** – This objective assessed controls designed to protect information as it moves across networks, systems, and communication channels, including encryption of sensitive data, secure authentication, firewall governance, and boundary protections. Audit testing verified whether transmission practices prevent unauthorized disclosure and maintain confidentiality and integrity during data movement.
- **Data in Use** – This objective evaluated the agency mechanisms that ensure information remains protected while actively processed, accessed, or manipulated within systems. This included reviewing integrity-checking tools, change management procedures, separation of development and production environments, and ongoing monitoring to detect unauthorized changes or data corruption during active use.

The Office of the Chief Inspector General worked in consultation with a cybersecurity vendor to develop the audit program guide. The audit program guide was also reviewed by participating agency Offices of Inspector General staff with special knowledge of cybersecurity audit techniques in the audit topic selected. Throughout the course of the audit, 11 one-hour training sessions were provided on the audit topic with Offices of Inspector General staff members throughout the enterprise in attendance. This training covered all elements of the audit program guide and was specifically focused on the four (4) fieldwork testing objectives.

The Office of the Chief Inspector General facilitated technical assistance and guidance to Offices of Inspector General staff regarding the audit throughout the entirety of the engagement. This included the facilitation of Microsoft Teams meetings every two (2) weeks after the conclusion of training sessions to discuss the audit topic, and any concerns audit staff members may have had with the specific elements of testing in this area.

The Office of the Chief Inspector General shared the Cyber Audit Program Guide in advance and launched it at an Enterprise Security Leaders' Meeting, hosted by FLDS to

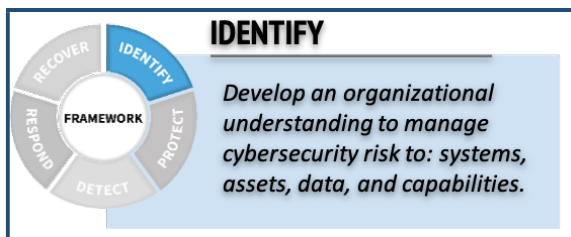


Executive Office of the Governor
Office of the Chief Inspector General
Annual Report FY 2025-2026

empower the agencies to self-evaluate, strengthen controls, and prepare for the audit ahead of time – turning the process into a collaborative opportunity for readiness, rather than a reactive exercise.

Department of Management Services, FLDS rules (Chapter 60GG-2, F.A.C.) establish minimum security standards for ensuring the confidentiality, integrity, and availability of state data, information, and information technology resources, referred to as the Florida Cybersecurity Standards. These rules are implemented by the NIST CSF.

NIST CSF v1.1 is comprised of five (5) high-level functions: Identify, Protect, Detect, Respond, and Recover. Under these high-level functions are underlying categories and subcategories. The purpose of the audit was to evaluate the relevant controls and compliance with the Identify (ID) and Protect (PR) high-level functions throughout the enterprise.



NIST Cybersecurity Framework

Function Identifier	Function	Category Identifier	Category
ID	Identify	ID.AM	Asset Management
		ID.BE	Business Environment
		ID.GV	Governance
		ID.RA	Risk Assessment
		ID.RM	Risk Management Strategy
		ID.SC	Supply Chain Risk Management
PR	Protect	PR.AC	Identity Management and Access Control
		PR.AT	Awareness and Training
		PR.DS	Data Security
		PR.IP	Information Protection Processes and Procedures
		PR.MA	Maintenance
		PR.PT	Protective Technology
DE	Detect	DE.AE	Anomalies and Events
		DE.CM	Security Continuous Monitoring
		DE.DP	Detection Processes
RS	Respond	RS.RP	Response Planning
		RS.CO	Communications
		RS.AN	Analysis
		RS.MI	Mitigation
		RS.IM	Improvements
RC	Recover	RC.RP	Recovery Planning
		RC.IM	Improvements
		RC.CO	Communications

Selected Categories
for FY 2025-2026



**Executive Office of the Governor
Office of the Chief Inspector General
Annual Report FY 2025-2026**

The three (3) NIST subcategories under the Identify function are as follows:

- Identify – Governance (ID.GV-1): Organizational cybersecurity policy is established and communicated.
- Identify – Governance (ID.GV-3): Legal and regulatory requirements regarding cybersecurity, including privacy and civil liberties obligations, are understood and managed.
- Identify – Risk Assessment (ID.RA-1): Asset vulnerabilities are identified and documented.

The eight (8) NIST subcategories under the Protect function are as follows:

- Protect – Data Security (PR.DS-1): Data at rest is protected.
- Protect – Data Security (PR.DS-2): Data in transit is protected.
- Protect – Data Security (PR.DS-3): Assets are formally managed throughout removal, transfers, and disposition.
- Protect – Data Security (PR.DS-4): Adequate capacity to ensure availability is maintained.
- Protect – Data Security (PR.DS-5): Protections against data leaks are implemented.
- Protect – Data Security (PR.DS-6): Integrity checking mechanisms are used to verify software, firmware, and information integrity.
- Protect – Data Security (PR.DS-7): The development and testing environment(s) are separate from the production environment.
- Protect – Data Security (PR.DS-8): Integrity checking mechanisms are used to verify hardware integrity.

All state agencies were invited to participate and results of these individual internal audits were issued by the Offices of Inspector General. A roll-up report was released September 1, 2026.

Asset Management – FY 2024-2025

The audit topic for the enterprise cybersecurity audit engagement for FY 2024-2025 was Asset Management. This enterprise audit evaluated the six (6) Identify – Asset Management subcategories (ID.AM-1 through ID.AM-6) under NIST CSF v1.1, as outlined in Rule 60GG-2.002(1), F.A.C.

The purpose of these audits was to evaluate agency controls and compliance with asset management requirements. The scope of these audits included an evaluation of agency cybersecurity policies, procedures, activities, and processes related to information system asset management. In addition to compliance, agency controls were evaluated to determine cybersecurity maturity specific to the three (3) audit testing



**Executive Office of the Governor
Office of the Chief Inspector General
Annual Report FY 2025-2026**

objectives, which were Asset Identification, Asset Classification and Categorization, and Asset Ownership and Responsibility.

All state agencies were invited to participate. The 20 participating agencies issued 84 findings and 140 recommendations for corrective action, all of which were provided to agency management for review and comment. A roll-up report summarizing the result of these asset management cybersecurity audits was released by the Office of the Chief Inspector General on September 12, 2025.

FY 2025-2026 Enterprise Cybersecurity Risk Assessment and FY 2026-2027 Enterprise Cybersecurity Audit Topic Development

As part of the FY 2024-2025 enterprise cybersecurity audit planning, a workgroup was created and tasked by the Chief Inspector General to assess potential cybersecurity and information technology risks to state agencies. The results of this assessment were used to support the recommendation for an enterprise cybersecurity audit topic for consideration by the Chief Inspector General.

The Office of the Chief Inspector General, together with the statewide Inspector General Cyber Workgroup, conducted an extensive research and risk assessment process to identify the FY 2026-2027 enterprise cybersecurity audit topic. This methodology incorporated reviews of statutory requirements under § 282.318, F.S., evaluations of Florida Cybersecurity Standards (Rule 60GG-2, F.A.C.), analyses of Auditor General Information Technology audit findings, 2023 triennial cybersecurity risk assessment results, and statewide Agency Strategic Operation Plan (ASOP) submissions. The Office of the Chief Inspector General also gathered updated remediation documentation from the FLDS and obtained input from state agency Chief Information Officers, Chief Information Security Officers, Information Security Managers, Inspector General staff, and internal auditors. These activities ensured the methodology reflected both regulatory expectations and real-time statewide cyber conditions.

Insights from key stakeholders significantly shaped the audit topic selection. FLDS leadership emphasized systemic enterprise risks, such as identity and access management weaknesses, escalating social engineering threats, and concerns related to unsecured virtual private network configurations. Practitioners across multiple agencies further highlighted operational challenges surrounding vendor oversight, especially in contracts lacking audit provisions, and stressed the value of focusing on training and detection-related controls. Risk analysis showed that several NIST CSF v1.1 categories, specifically Supply Chain Risk Management (ID.SC) and detection-related domains (DE.AE and DE.DP), contained subcategories frequently rated High or Very High across agencies, including multiple core controls identified in the triennial cybersecurity risk assessment. This convergence of statewide risk trends,



Executive Office of the Governor
Office of the Chief Inspector General
Annual Report FY 2025-2026

operational feedback, and prior audit coverage highlighted supply chain-related vulnerabilities as a significant enterprise-level concern.

On April 20, 2026, the Chief Inspector General selected Supply Chain Risk Management (ID.SC-1 through ID.SC-5) as the FY 2026-2027 enterprise cybersecurity audit topic. The chosen focus reflects a strategic shift toward evaluating the state's ability to detect and respond to trusted-pathway compromises, particularly those originating from third-party vendors, identity-based access, and integrated systems. The Office of the Chief Inspector General recognized that the most critical risk is not merely that a vendor may be compromised, but that the state may not detect or respond in time to prevent harm. In addition to the audit, the Office of the Chief Inspector General will engage a vendor to perform Ground Truth Testing across detection and access-control domains (DE.AE, DE.DP, selected PR.AC) in high-risk agencies and systems. This hybrid approach, combining targeted NIST subcategory audits with enterprise-level testing, supports a more comprehensive and risk-aligned statewide cybersecurity posture.

For the enterprise cybersecurity audit topic of Supply Chain Risk Management, an audit program was developed by a cybersecurity vendor and disseminated to agency Offices of Inspector General staff in June 2026.

Cybersecurity Technical Assistance – Ground Truth and Ad Hoc Testing

The Ground Truth Cybersecurity and Ad Hoc Testing initiative, conducted during FY 2025-2026, represented a major statewide effort by the Office of the Chief Inspector General, working in conjunction with agency Offices of Inspector General and a selected vendor, to review the effectiveness of cybersecurity controls implemented across participating Florida agencies. Please note, however, agency Offices of Inspectors General remained responsible for their audit conclusions separate from this ground truth and ad hoc testing initiative. A total of 12 executive branch state agencies participated in this project.

Supported by a cybersecurity vendor, the project provided an end-to-end technical assessment of selected cybersecurity safeguards, including data protection, encryption, access control, monitoring, and overall compliance with the Florida Cybersecurity Standards. Through both Enterprise Testing and Ad Hoc Testing, the initiative produced actionable insights into control performance, vulnerability exposure, and opportunities for improving operational cybersecurity practices across diverse systems and environments.

The comprehensive methodology used for this initiative combined structured test planning, detailed evidence collection, technical testing, scenario-based ground truth validation, and quality assurance in which the vendor provided the evidence of their



**Executive Office of the Governor
Office of the Chief Inspector General
Annual Report FY 2025-2026**

testing conclusions with agency Offices of Inspector General and Information Technology staff. The vendor assessment team reviewed evidence packages, logs, system configurations, and testing artifacts against secure baselines and relevant NIST CSF and NIST Special Publication 800-53 requirements. The initiative not only confirmed whether cybersecurity controls were present and configured correctly, but also whether they performed effectively when exposed to simulated threats or defined behavioral conditions.

However, vendor technical ground truth and ad hoc testing were conducted separately from the independent audit testing and conclusions reached by agency Inspectors General regarding the data protection and security control environment as part of the enterprise cybersecurity audit conducted in Fiscal Year 2025-2026. While vendor testing provided initial insights into system security, independent audit testing by agency Inspectors General offered an unbiased evaluation, ensuring comprehensive oversight of data protection measures. Together, these approaches complement each other by combining practical evidence from vendors with impartial assessments, resulting in a more robust review of statewide cybersecurity practices.

All deliverables and test results were coordinated through agency Offices of Inspector General, with the Office of the Chief Inspector General maintaining oversight to ensure consistency, transparency, and adherence to statewide governance expectations.

Across agencies, ground truth testing observations throughout the enterprise included inconsistent control implementation, detectable vulnerabilities, gaps in compliance with technical configuration standards, and opportunities to enhance system monitoring and automated enforcement mechanisms. These findings provided agencies with actionable recommendations to improve risk management practices and strengthen alignment with statewide cybersecurity expectations. The project also brought forward important enterprise-level observations that will inform future oversight decisions, including systemic trends in logging practices, configuration management, and detection effectiveness.

The project also included a formal documentation of lessons learned. These included the importance of early scope alignment, standardized testing procedures, robust evidence management, improved coordination across agencies, and integrated policy-technical validation. The selected vendor's deliverables emphasized the value of consistent stakeholder communication, repeatable testing frameworks, and clearer reporting structures that facilitate decision-making by both the Office of the Chief Inspector General and agency leadership. These lessons create a foundation for more efficient and reliable statewide technical assessment efforts in future years.

All contractual deliverables were successfully completed and accepted, with final project approval issued on June 30, 2026.



**Executive Office of the Governor
Office of the Chief Inspector General
Annual Report FY 2025-2026**

Proof of Concept for Data Analytics Tool for Anomaly Detection

The Office of the Chief Inspector General successfully completed the Data Analytics Tool for Anomaly Detection Proof of Concept (POC) in June 2026, marking a significant step toward modernizing statewide oversight through data-driven methods. The initiative explored whether advanced analytics could strengthen the state's ability to identify unusual procurement and financial activity, such as irregular payments, data inconsistencies, or emerging patterns more efficiently and at an enterprise scale. The Office of the Chief Inspector General worked with a selected vendor to evaluate a secure analytical platform capable of integrating data from Florida's major procurement and financial systems and producing screening indicators, known as Items for Further Review, to support oversight and audit planning.

Across the POC, the vendor successfully integrated key statewide data sources, including procurement data from MyFloridaMarketPlace (MFMP) and financial records from Florida Accounting Information Resource (FLAIR) and FACTS. The POC further demonstrated that data could be securely integrated, normalized, and analyzed using modern tools. The resulting platform produced outputs using business-rule-based anomaly detection and intuitive dashboards that aligned with the Office of the Chief Inspector General's oversight workflows. The POC confirmed that meaningful insights can be derived even when data comes from systems with differing formats or levels of maturity, underscoring the importance of improving statewide data quality and standardization as Florida moves toward more automated oversight capabilities.

The effort also highlighted several important lessons. The Office of the Chief Inspector General identified the need for consistent data governance, stronger cross-system identifiers, and improved completeness across procurement and financial records to maximize future analytical value. Early stakeholder engagement, clear business-rule design, and disciplined validation proved essential to ensuring reliable results. These findings reinforced the Office of the Chief Inspector General's view that data analytics can significantly enhance visibility and accountability, but must be paired with structured governance, clear responsible-use principles, and human judgment. All system outputs generated by the POC were explicitly presented as indicators rather than findings, preserving the integrity of Inspector General review and investigative decision-making.

From an enterprise perspective, the POC demonstrated that modern analytics can help Florida strengthen oversight by reducing manual data review, improving cross-system visibility, and enabling faster identification of potential issues. The architecture proved scalable and flexible, capable of incorporating additional statewide systems as they evolve, and adaptable enough to support broader oversight domains in the future. The Office of the Chief Inspector General now possesses a complete suite of state-owned deliverables, including rule logic, models, documentation, and dashboards, enabling the state to build upon the POC without vendor dependence.



**Executive Office of the Governor
Office of the Chief Inspector General
Annual Report FY 2025-2026**

The POC's successful completion on June 30, 2026, provides a strong foundation for future modernization. As Florida continues to strengthen accountability and transparency, the insights gained from this POC will directly inform future planning, potential enterprise expansion, and continued investment in data-driven oversight strategies.

Additional Office of the Chief Inspector General Cybersecurity Activities

During FY 2025-2026, the Office of the Chief Inspector General also participated in the following cybersecurity activities:

- Three (3) members of the Office of the Chief Inspector General served as part of the Govern and Identify workgroup within FLDS. This group focuses on enterprise-wide governance, risk management, and the identification of cybersecurity risks and assets. The workgroup works to develop policies, frameworks, and templates that ensure agencies understand their cyber environment and associated risks.
- One Office of the Chief Inspector General staff member serves as part of the Respond and Recover FLDS workgroup. This group focuses on enhancing the state's ability to respond to and recover from cybersecurity incidents. By developing and refining incident response processes, after-action reporting, and recovery strategies, the group aims to ensure agencies are well-prepared to manage incidents effectively and resume operations quickly and securely.
- Office of the Chief Inspector General staff attended multiple Enterprise Cybersecurity Leaders meetings held by FLDS. These monthly operational meetings and collaborative discussions are designed for enterprise security leaders and public-sector CISOs and focus on state agency governance, risk mitigation, and security compliance.
- The Office of the Chief Inspector General coordinated participation of state agency Inspectors General staff, who functioned as non-technical observers for Computer Security Incident Response Team (CSIRT) exercises at all 35 participating agencies, evaluating the communication efforts of agency CSIRT teams. In accordance with § 282.318(3)(e), F.S., FLDS is responsible for annually providing training for state information security managers and CSIRT members that contains training on cybersecurity, including cybersecurity threats, trends, and best practices.
- The Chief Inspector General also serves as a statutory appointee to the Florida Cybersecurity Advisory Council (CAC). The CAC protects state technology resources, advises state and local governments on cybersecurity trends, and assists FLDS with security standards. The CAC is also responsible for submitting annual legislative recommendations to state leaders by June 30 of each fiscal year.



Executive Office of the Governor
Office of the Chief Inspector General
Annual Report FY 2025-2026

Cybersecurity Training for Offices of Inspector General

In FY 2025-2026, the General Appropriations Act appropriated \$1 million in funding to the Office of the Chief Inspector General to support enterprise cybersecurity resiliency. As a result, the Office of the Chief Inspector General implemented a multi-featured Cyber Pathways Program to support agency Offices of Inspector General. This program is designed to create “pathways” to cyber competency and address the requirements for the specific annual cyber audit plan required by law. The program includes training, tools, and audit enablement.

The Cyber Pathways Program ensures that Offices of Inspector General staff are equipped with the essential tools and knowledge to audit, investigate, inspect, and assess cybersecurity practices. The program enables staff to review cybersecurity risk management, assess agency compliance with government requirements such as NIST, and follow professional auditing and investigative standards.

Nineteen (19) separate classes and workshops were developed and delivered to 309 state and local personnel throughout our Cyber Pathways Program to promote awareness of cybersecurity tools to detect fraud and manage internal controls, risk management, and compliance. A total of 3,671 hours of training were provided to relevant attendees.

In addition, three (3) separate Certified Internal Auditor® (CIA) Exam Preparation Courses, presented in partnership with the IIA Tallahassee Chapter and Becker Professional Development Corporation, were offered as part of our Cyber Pathways Program and associated funding. This CIA Exam includes understanding of information security controls in alignment with our Cyber Pathways Program goal to create skilled auditors prepared to meet Florida’s complex oversight and cybersecurity challenges.

Benefits of all of these training sessions included more effective cybersecurity audits and investigations, reduced need for staff augmentation to perform cybersecurity audits, more strategic awareness of agency information technology operations, and an enhanced skillset for agency Offices of Inspector General staff.

Specific cybersecurity training for FY 2025-2026 included the following:

Training	Date Completed
Artificial Intelligence Competency Workshop	July 29, 2025
Cyber Forensics Investigator Training	September 18, 2025
Certified Information System Auditor (CISA) TM Training	October 6, 2025



**Executive Office of the Governor
Office of the Chief Inspector General
Annual Report FY 2025-2026**

Training	Date Completed
CIA™ Training – Part One	November 18, 2025
Cybersecurity Audit Topical Requirements Training Session	November 19, 2025
CIA™ Training – Part Two	March 4, 2026
Data Protection and Security Training (11 real-time learning sessions)	April 9, 2026
ISACA Advanced in Artificial Intelligence Audit Certification Training	May 11, 2026
CIA™ Training – Part Three	May 13, 2026
eDiscovery Investigative Training Sessions (3 real-time training sessions)	May 20, 2026

In addition to these classes, the Office of the Chief Inspector General maintained an email inbox, known as the “Ask the CIG Mailbox” or CIG_CyberAudits Mailbox, in which agencies submit various inquiries regarding cybersecurity issues encountered. The bulk of the inquiries received concerned specific requests to aid internal audit staff in the completion of the enterprise cybersecurity audit of Asset Management. However, other inquiries concerning cybersecurity investigations and general information technology control risks were also submitted. The Office of the Chief Inspector General partnered with a cybersecurity vendor to respond to these inquiries and disseminate a response to the requesting agency within three (3) business days.

Accreditation

Section 943.125, F.S., outlines that certain agencies of the state, including state and local law enforcement agencies, correctional facilities, public agency Offices of Inspector General, and certain pretrial diversion programs “be upgraded and strengthened through the adoption of meaningful standards of operation for those agencies and their functions.” This statute further indicates that the intent of this section, in part, for public agency Offices of Inspector General, is “to promote more effective scrutiny of public agency operations and greater accountability of those serving in those agencies.” In 2007, the Chief Inspector General appeared before the Commission for Florida Law Enforcement Accreditation (Commission) during their executive workshop to inquire about developing an accreditation program for Offices of Inspector General. In October 2007, the Commission approved the development of an accreditation program.

The Office of the Chief Inspector General’s investigative function was initially accredited by the Commission on February 25, 2015, and most recently reaccredited on February



**Executive Office of the Governor
Office of the Chief Inspector General
Annual Report FY 2025-2026**

22, 2024. During FY 2025-2026, the Office of the Chief Inspector General and agency Inspectors General, in collaboration with the Commission, continued efforts to enhance compliance with the *Principles and Standards for Offices of Inspector General*, as published and revised by the Association of Inspectors General, through the advancement and support of the Office of Inspector General accreditation program.

The following Offices of Inspector General earned or retained accredited status from the Commission during the fiscal year: Agency for Healthcare Administration Office of Inspector General, Attorney General Office of Inspector General, Department of Business and Professional Regulation Office of Inspector General, Department of Education Office of Inspector General, Florida Department of Elder Affairs Office of Inspector General, Florida Department of Law Enforcement Office of Inspector General, Florida Division of Emergency Management Office of Inspector General, Florida Housing Finance Corporation Office of Inspector General, Florida Office of Financial Regulation Office of Inspector General, Florida Office of Insurance Regulation Office of Inspector General, Florida Lottery Office of Inspector General, Okaloosa County Clerk of the Circuit Court Department of Inspector General, and the State University System Board of Governors Office of Inspector General.

In addition, the Florida Department of Highway Safety and Motor Vehicles Office of Inspector General earned Excelsior status from the Commission during the fiscal year.

Global Internal Audit Standards Update

The new *Global Internal Audit Standards* were released by the IIA on January 9, 2024. The *Global Internal Audit Standards* guide the worldwide professional practice of internal auditing and serve as a basis for evaluating the quality of the internal audit function. At the heart of the *Global Internal Audit Standards* are 15 guiding principles that enable effective internal auditing.

The *Global Internal Audit Standards* were significantly revised to include topical requirements and revised guidance concerning internal audit processes and activities. The *Global Internal Audit Standards* became effective January 9, 2025.

To provide guidance to agency Offices of Inspector General, the Office of the Chief Inspector General set up a working group and held numerous meetings throughout FY 2025-2026, including three separate in-person roundtable meetings with state agency Directors of Auditing, to guide staff on these changes and collaboratively prepare staff for upcoming external quality assurance reviews.

External Quality Assurance Review (QAR) – Audit

During 2026, the Auditor General completed an independent External QAR of the Executive Office of the Governor's Office of the Chief Inspector General internal audit



**Executive Office of the Governor
Office of the Chief Inspector General
Annual Report FY 2025-2026**

activity, covering the period January 2025 through December 2025. The Auditor General conducted the review pursuant to § 11.45(2)(i), F.S., which requires the Auditor General to assess a sample of internal audit work every three years to ensure conformance with professional auditing standards. The assessment team, led by certified public accountants, evaluated the Office of the Chief Inspector General's mandate, charter, governance, methodologies, performance measures, and adherence to statutory requirements governing internal audit activities.

The Auditor General found the Office of the Chief Inspector General internal audit activity to fully conform with applicable professional auditing standards, specifically the *Global Internal Audit Standards* issued by the IIA. The review further confirmed that the Office of the Chief Inspector General fully achieved the principles and purpose of internal auditing, demonstrating high-quality practices in assurance engagements, risk assessment, professional development, and audit governance. This independent validation affirms that the Office of the Chief Inspector General's internal audit processes are robust, professionally sound, and aligned with national and international standards.

In addition to confirming standards conformance, the review found that the Office of the Chief Inspector General generally complied with § 20.055, F.S., which governs the operation of agency-level Offices of Inspectors General. The Auditor General's methodology followed the IIA's Quality Assessment Manual, incorporating interviews, documentation review, workpaper evaluation, and testing of audit processes. The review team examined one assurance engagement substantially completed during the period and confirmed that it met the relevant professional standards. While the report emphasized inherent limitations associated with any Quality Assurance and Improvement Program (QAIP), it concluded that the Office of the Chief Inspector General's program is operating effectively, with no departures from standards identified during the review period.

Overall, this external assessment provides strong assurance that the Office of the Chief Inspector General maintains a mature, compliant, and high-performing internal audit function. By fully conforming to professional standards and meeting statutory obligations, the Office of the Chief Inspector General continues to provide reliable, independent oversight that supports accountability, integrity, and operational excellence within the Executive Office of the Governor.

Internal QAR – Audit

During FY 2025-2026, the Office of the Chief Inspector General conducted an Internal QAR to evaluate the extent to which its internal audit activities conform to the *Global Internal Audit Standards* issued by the IIA. This self-assessment, required under both the *Global Internal Audit Standards* and § 20.055, F.S., reflects the Office of the Chief



**Executive Office of the Governor
Office of the Chief Inspector General
Annual Report FY 2025-2026**

Inspector General's commitment to maintaining a strong, standards-aligned internal audit function.

The QAR concluded that the Office of the Chief Inspector General's internal audit activity operates in full conformance with the *Global Internal Audit Standards*, reinforced by the recent external QAR conducted by the Auditor General, as described above.

While the Office of the Chief Inspector General's audit activity met all required standards, the QAR identified several opportunities to further enhance audit practices. These include updating staff training plans to align with the IIA's newly released Internal Auditing Competency Framework, integrating emerging IIA Topical Requirements, such as Third-Party, Organizational Behavior, and Organizational Resilience, into audit planning, and documenting instances where AI is used in audit workpapers to promote transparency and responsible innovation. These targeted improvements reflect the Office of the Chief Inspector General's continued leadership in applying best practices across public-sector internal audit functions.

The review also acknowledged the unique governance context of state government, where the Governor serves as the functional equivalent of an audit committee or board. Despite structural differences from private-sector audit governance, the Office of the Chief Inspector General has implemented appropriate compensating measures, such as the Domain III briefing book, to ensure meaningful communication consistent with the *Global Internal Audit Standards*. This adaptability demonstrates the Office of the Chief Inspector General's commitment to maintaining a robust and fully compliant QAIP.

Overall, the FY 2025-2026 QAR confirmed that the Office of the Chief Inspector General's internal audit activity remains effective, compliant, and aligned with evolving professional standards. The improvements identified during the review will be implemented by September 1, 2026, strengthening the internal audit function and reinforcing the Office of the Chief Inspector General's position as a leader in public-sector audit excellence. The results were formally transmitted to the Governor on June 25, 2026, ensuring transparency and accountability in accordance with statutory and professional requirements.



Executive Office of the Governor
Office of the Chief Inspector General
Annual Report FY 2025-2026

INVESTIGATIVE ACTIVITY

Investigations often begin with allegations received by telephone, letter, fax, website, or email.⁶ Additionally, in accordance with §§ 112.3187 - 112.31895, F.S., Florida's Whistle-blower's Act, the Office of the Chief Inspector General maintains a statewide Whistle-blower's Hotline, where employees of the state or contracted providers may disclose allegations of gross mismanagement, gross waste of public funds, malfeasance, misfeasance, gross neglect of duty, or other activities covered by Florida's Whistle-blower's Act.

During FY 2025-2026, the Office of the Chief Inspector General received 4,651 complaints or requests for assistance from various sources, as follows:

FY 2025-2026 Complaints or Requests by Source

FY 2025-2026 Correspondence by Origin	Count
Web Site	619
Whistle-blower Hotline	392
Referral IG	119
Email	1,626
Phone	1,545
Mail	232
Referral Other	66
Fax	28
Walk-in	24 ⁷
Total	4,651

All complaints and requests for assistance were documented in the Office of the Chief Inspector General database. During the fiscal year, 4,608 complaints and requests were closed.

The Office of the Chief Inspector General received, reviewed, and processed 4,203 correspondence containing additional information related to existing correspondence during the fiscal year as follows:

⁶ According to *Occupational Fraud 2026: A Report to the Nations*, published by the Association of Certified Fraud Examiners (ACFE), tips remain the top source of fraud detection, particularly from employees, customers, or vendors (43%), followed by internal audit (15%), management review (13%), document examinations (5%), account reconciliation (5%), other (5%), by accident (4%), data monitoring (3%), external audit (2%), surveillance (2%), notification by law enforcement (2%), and confession (1%).

⁷ Of the 24 walk-in complaints, 22 were based on interviews conducted in conjunction with an ongoing Office of the Chief Inspector General investigation.



Executive Office of the Governor
Office of the Chief Inspector General
Annual Report FY 2025-2026

FY 2025-2026 Additional Information by Source

FY 2025-2026 Additional Information by Origin		Count
Web Site		98
Whistle-blower Hotline		0
Referral IG		404
Email		2,854
Phone		584
Mail		98
Referral Other		113
Fax		50
Walk-in		2
Total		4,203

FY 2025-2026 Summary of Complaint Activity by Quarter

	Q1	Q2	Q3	Q4	Total
Number of Complaints and Requests Opened	1,321	1,078	1,067	1,185	4,651
Number of Complaints and Requests Closed	1,305	1,088	1,054	1,161	4,608
Number of Whistle-blower Hotline Calls Received	128	84	102	78	392
Number of Complaints Referred to Other Entities	345	276	300	350	1,271

Investigative Highlights

In addition to the Office of the Chief Inspector General projects previously listed, the following case summaries provide an overview of other investigations, reviews, or activities in which the Office of the Chief Inspector General played a role during this fiscal year.



**Office of the Chief Inspector General
Correspondence #2025-07-14-0012**

On July 14, 2025, the Office of the Chief Inspector General received a complaint about potential misconduct within the Florida Department of Corrections (FDC) Office of Inspector General Region 2 East Criminal Investigation Bureau. As a result, the Office of the Chief Inspector General initiated an inquiry to determine if an investigation was warranted. The Office of the Chief Inspector General determined that sufficient information was provided by the FDC Inspector General to indicate that no violations of law, rule, policy, or procedure occurred; therefore, a full investigation was not warranted by the Office of the Chief Inspector General. This matter was closed on September 23, 2025.



**Executive Office of the Governor
Office of the Chief Inspector General
Annual Report FY 2025-2026**

**Office of the Chief Inspector General
Correspondence #2025-09-19-0015**

On September 19, 2025, the Office of the Chief Inspector General received a complaint from the Florida Department of Law Enforcement (FDLE) Office of Executive Investigations regarding a complaint they were forwarded from the Florida Fusion Center's Intelligence Watch and Warning Desk, in which the complainant expressed concerns about the conduct of staff within the FDC Office of Inspector General. As a result, the Office of the Chief Inspector General initiated an inquiry to determine if an investigation was warranted. The Office of the Chief Inspector General determined that sufficient information was provided by the FDC Inspector General to indicate that no violations of law, rule, policy, or procedure occurred; therefore, a full investigation was not warranted by the Office of the Chief Inspector General. This matter was closed on October 24, 2025.

**Office of the Chief Inspector General
Correspondence #2025-10-22-0009**

On October 22, 2025, the Office of the Chief Inspector General received a complaint about the handling of an FDC Office of Inspector General investigation and the conduct of FDC Office of Inspector General staff. As a result, the Office of the Chief Inspector General initiated an inquiry to determine if an investigation was warranted. The Office of the Chief Inspector General determined that sufficient information was provided by the FDC Inspector General to indicate that no violations of law, rule, policy, or procedure occurred; therefore, a full investigation was not warranted by the Office of the Chief Inspector General. This matter was closed on March 12, 2026.

**Office of the Chief Inspector General
Correspondence #2025-12-12-0016**

On December 12, 2025, the Office of the Chief Inspector General received a complaint about a Florida Gaming Control Commission (FGCC) contract. As a result, the Office of the Chief Inspector General initiated an inquiry and coordinated with the FGCC Office of Inspector General to determine if an investigation was warranted. The Office of the Chief Inspector General and FGCC Office of Inspector General determined that sufficient information was provided by the FGCC Board Chair to indicate that no violations of law, rule, policy, or procedure occurred; therefore, a full investigation was not warranted by the Office of the Chief Inspector General. This matter was closed on June 17, 2026.



**Executive Office of the Governor
Office of the Chief Inspector General
Annual Report FY 2025-2026**

**Office of the Chief Inspector General
Correspondence #2026-03-22-0006**

On March 22, 2026, the Office of the Chief Inspector General received a complaint about the handling of an FDLE Office of Inspector General investigation. As a result, the Office of the Chief Inspector General initiated an inquiry to determine if an investigation was warranted. The Office of the Chief Inspector General determined that sufficient information was provided by the FDLE Inspector General to indicate that no violations of law, rule, policy, or procedure occurred; therefore, a full investigation was not warranted by the Office of the Chief Inspector General. This matter was closed on June 3, 2026.

**Office of the Chief Inspector General
Correspondence #2026-04-01-0008**

On April 1, 2026, the Office of the Chief Inspector General received a complaint about the Department of Juvenile Justice (DJJ) Office of Inspector General. As a result, the Office of the Chief Inspector General initiated an inquiry to determine if an investigation was warranted. The Office of the Chief Inspector General determined that sufficient information was provided by the DJJ Inspector General to indicate that no violations of law, rule, policy, or procedure occurred; therefore, a full investigation was not warranted by the Office of the Chief Inspector General. This matter was closed on June 3, 2026.

**Office of the Chief Inspector General
Correspondence #2026-05-07-0009**

On May 7, 2026, the Office of the Chief Inspector General received a complaint about the conduct of staff with the Executive Office of the Governor, Department of Education, Department of Elder Affairs, Department of Management Services, and Division of Emergency Management. As a result, the Office of the Chief Inspector General initiated an inquiry to determine if an investigation was warranted. The Office of the Chief Inspector General determined that sufficient information was provided by agency staff to indicate that no violations of law, rule, policy, or procedure occurred; therefore, a full investigation was not warranted by the Office of the Chief Inspector General. This matter was closed on June 17, 2026.

Summary of Whistle-blower Activity

During FY 2025-2026, the Office of the Chief Inspector General coordinated and oversaw the processing of whistle-blower determinations and investigations in accordance with Florida's Whistle-blower's Act. The Office of the Chief Inspector General ensured a consistent assessment process for applying statutory requirements by agency Inspectors General and provided coordination and oversight of investigative activities involving the most serious allegations.



**Executive Office of the Governor
Office of the Chief Inspector General
Annual Report FY 2025-2026**

During the fiscal year, agency Inspectors General completed 195 whistle-blower determinations in accordance with the provisions of §§ 112.3187 - 112.31895, F.S., Florida's Whistle-blower's Act. Of those determinations, 13 met the statutory provisions to be designated as a whistle-blower complaint. Additionally, agency Inspectors General completed three (3) whistle-blower investigations.

The Office of the Chief Inspector General monitored each investigation until completion for compliance with statutory timeframes and granted extensions for good cause when circumstances warranted, in accordance with § 112.3189, F.S. As required by § 112.3189(8)(e)4., F.S., the FDLE was notified of any whistle-blower cases that produced evidence of criminal violations. Finally, all investigative reports were submitted to and independently reviewed by the Office of the Chief Inspector General for investigative sufficiency prior to final release. These reports were distributed as required by § 112.3189, F.S.

Whistle-blower Case Highlights

The following case summaries represent examples of the types of investigations conducted and finalized in accordance with the Florida Whistle-blower's Act.

Department of Environmental Protection

CIG Correspondences #2022-01-04-0007 and #2022-01-19-0008

On January 19, 2022, the Office of Inspector General for the Department of Environmental Protection initiated a whistle-blower investigation to address concerns about oversight of the Water Supply Restoration Funding Program by staff and citizens drinking contaminated water. The allegation was "not substantiated."

Department of Children and Families

CIG Correspondence #2024-06-04-0009 and #2024-07-15-0004

On June 10, 2024, the Office of Inspector General for the Department of Children and Families initiated a whistle-blower investigation to address the conduct of staff with the Department of Children and Families, Florida State Hospital. The Office of Inspector General determined that the potential for the investigation to yield further recommendations to make state government more efficient and effective was moot, therefore, the investigation was terminated prior to completion and the Office of Inspector General made no finding.



**Executive Office of the Governor
Office of the Chief Inspector General
Annual Report FY 2025-2026**

**Department of Transportation
CIG Correspondence #2024-10-30-0010**

On October 28, 2024, the Office of Inspector General for the Department of Transportation initiated a whistle-blower investigation to address concerns about a Department of Transportation contracted agency, DeAngelo Contracting Services, LLC. Of the two allegations, one was “proved” and the other “inconclusive.”

Summary of Subpoena Activity

During FY 2025-2026, in accordance with § 14.32(5), F.S., the Office of the Chief Inspector General did not issue any subpoenas.

AUDIT ACTIVITY

In accordance with § 14.32, F.S., and § 20.055, F.S., the Office of the Chief Inspector General is responsible for carrying out auditing duties and reviewing, evaluating, and monitoring the policies, practices, and operations of the Executive Office of the Governor. In addition, § 20.055(2), F.S., includes a description of activities related to the development, assessment, and validation of performance measures. These activities are integrated into the audit process, if applicable. During FY 2025-2026, the Office of the Chief Inspector General conducted internal audits, provided audit assistance to other agency Inspectors General, and monitored the status of internal and external corrective actions recommended in audits as follows:

Executive Office of the Governor, Audit of Mail Room Processes and Internal Controls - EOG, Audit Report #A-2526-002

Pursuant to the Office of the Chief Inspector General’s FY 2025-2026 Audit Plan, the Office of the Chief Inspector General conducted an assurance audit of the Executive Office of the Governor’s mail room and supply room operations for FY 2025-2026. The purpose of the audit was to evaluate internal controls related to mail security, handling processes, and inventory management. Overall, the review found that controls are generally effective, with two (2) security-related findings requiring corrective action. Auditors reviewed policies and procedures, interviewed staff, observed operations, and conducted testing against industry standards, including United States Postal Service (USPS) and General Services Administration (GSA) best practices.

The scope of the audit included policies, procedures, activities, and processes related to the mail and supply room. Our review encompassed records, transactions, and documentation for the period July 1, 2024 through June 30, 2025, and related activities through the conclusion of fieldwork in January 2026. The objective of this audit was to evaluate the sufficiency and effectiveness of internal controls governing the security,



**Executive Office of the Governor
Office of the Chief Inspector General
Annual Report FY 2025-2026**

receipt, handling, and processing of mail and supplies within the Executive Office of the Governor, including the integrated responsibilities of the mail room in managing supply room operations.

The audit concluded that internal controls over mail and supply rooms operations are generally strong and function effectively, with only two (2) areas requiring enhanced security measures and four recommendations issued. Management demonstrated responsiveness and a commitment to strengthening operational integrity through corrective actions.

Follow-up and Liaison Activities

During FY 2025-2026, the Office of the Chief Inspector General conducted both a six (6)-month and 12-month review of the status of corrective actions contained in Office of the Chief Inspector General Report #A-2425-001, *Enterprise Audit of the Executive Office of the Governor's Cybersecurity Controls for Asset Management*. After 12 months, the monitoring results disclosed that processes have been put in place to address the risk associated with the identified findings. However, additional time is needed to formalize and fully document these processes. As such, the Office of the Chief Inspector General will conduct additional monitoring no later than December 2026.

Additionally, and in accordance with § 20.055(2), F.S., the Office of the Chief Inspector General served as liaison between the Executive Office of the Governor and the Auditor General or other oversight bodies on projects related to the Executive Office of the Governor. Notably, in FY 2025-2026, this included the Auditor General 2025 *Operational Audit of the Executive Office of the Governor* (not yet completed) with an engagement letter issued on April 18, 2025, and the Department of Financial Services review of Executive Office of the Governor contract management and monitoring processes for selected contract and grant agreements, with an engagement letter issued on May 4, 2026.



**Executive Office of the Governor
Office of the Chief Inspector General
Annual Report FY 2025-2026**

Audit Plan for FY 2026-2027

Section 20.055(6)(i), F.S., requires that annual and long-term audit plans be developed based on the findings of periodic risk assessments. Based on the results of a risk assessment, top priorities for audits, reviews, and special projects were identified and the audit plan for FY 2026-2027 was developed and approved by the Governor. The 6,240 staff hours available for audits and audit activities were allocated as follows:

Allocation of Staff Hours for FY 2026-2027		
Hours Available:	52 weeks x 40 hours per week x 3 positions [Full-time Equivalent (FTE)] – 6,240 available hours.	100%
Estimated Distribution of Available Hours without Overtime		
Internal Audits, Enterprise Projects, and Other Assurance Activities	Hours available for internal and enterprise-wide audits, advisory services, and management reviews. This includes the Internal QAR of the Executive Office of the Governor, Office of the Chief Inspector General's internal audit activity. See also, Domain V of the <i>Global Internal Audit Standards</i> . This category is estimated at 1,248 hours.	20%
Audit Follow-up	As required in § 20.055(6)(h), F.S., and Principle 15 of the <i>Global Internal Audit Standards</i> . This is estimated at 125 hours.	2%
Liaison Activities to Coordinate External Audits	As required by § 20.055(2)(g), F.S. - Office of Program Policy Analysis and Government Accountability's Audits - Auditor General's Statewide Financial, Operational, and Federal Awards Audits - Auditor General's QAR at Selected agency OIGs. - Auditor General Operational Audit of the Executive Office of the Governor See also, Standard 9. Of the <i>Global Internal Audit Standards</i> This is estimated at 125 hours.	2%
Technical Assistance	Hours to assist other offices as directed by the Chief Inspector General in accordance with § 14.32, F.S. In addition to Special Projects. This is estimated at 2,808 hours.	45%
Financial Emergency Activities	Hours for monitoring and liaison activities associated with Financial Emergencies in accordance with § 218.503, F.S. This is estimated at 62 hours.	1%
Recurring Projects	- Risk Assessment and Annual Work Plan as required by § 20.055(6)(i), F.S. See also, Standard 9.4 of the <i>Global Internal Audit Standards</i>. - Inclusion of cybersecurity audit plan as required by § 20.055(6)(i), F.S. - Annual Report as required by § 20.055(8)(a) and (b), F.S. This is estimated at 624 hours.	10%
Indirect Hours	Hours for administrative activities include training, leave, state holidays, etc. This is estimated at 1,248 hours.	20%
% of Total Hours		100%



Executive Office of the Governor
Office of the Chief Inspector General
Annual Report FY 2025-2026

Of the available staff hours for FY 2026-2027, the Office of the Chief Inspector General estimates that it will initiate the following assurance activities based on the periodic risk assessment:

Planned Projects		
Category	Description	Hours
Internal Audit	Executive Office of the Governor – Audit of the Office of Open Government. (189 hours x 2 Auditor FTEs + 70 hours of supervisory review)	448
Cyber Enterprise Project*	Enterprise Audit for Fiscal Year 2026-2027 is scheduled to be Supply Chain Risk Management. (325 hours x 2 Auditor FTEs + 150 hours of supervisory review)	800
Total Hours		1,560 ⁸

* This Cyber Enterprise Project also satisfies the requirements of § 20.055(6)(i), F.S., requiring that the annual audit plan also include a specific cybersecurity audit plan.

As part of our technical assistance hourly allocation for this fiscal year, the Office of the Chief Inspector General will dedicate 400 hours of staff time to the safe and responsible integration of AI into all our processes, including our audit process. All AI adoption is guided by good governance controls and best practices, ensuring full compliance with applicable standards and regulations. As part of the audit process, and in accordance with *Global Internal Audit Standard* 10.3, Technological Resources, auditors are required to proactively enhance their use of technology and expand their skill sets. The Office of the Chief Inspector General is leading an enterprise-wide effort to innovate audit processes and responsibly implement technology, including AI, in activities such as examining the risk environment, developing the audit plan, and reviewing the sufficiency of audit documentation. These efforts are designed to strengthen our audit capabilities while maintaining the highest standards of safety, oversight, and accountability as we embrace technological modernizations and advancements.

Long-Term Audit Plans for FY 2027-2028 and FY 2028-2029

For FY 2027-2028 and FY 2028-2029, we plan to conduct a detailed risk assessment to determine specific projects selected. However, we do allocate direct hours each year to audit activities that will include the following:

House Bill 1297, which passed in 2021, amended § 20.055(6)(i), F.S., and requires each agency inspector general to develop an annual specific cybersecurity audit plan. An enterprise cybersecurity risk assessment was conducted by the Office of the Chief Inspector General and several state agency Inspectors General to determine the Cyber Enterprise Project topic for FY 2026-2027 with the selected topic of Supply Chain Risk

⁸ This figure of 1,560 hours represents 25% of available staff hours for the fiscal year to be devoted to internal audits, enterprise projects, and other assurance activities as noted in our allocation of staff hours. Additional hours may be allocated, as needed, for management requests for assurance or advisory services not listed herein.



**Executive Office of the Governor
Office of the Chief Inspector General
Annual Report FY 2025-2026**

Management. An enterprise cybersecurity risk assessment will also be conducted to determine the Cyber Enterprise Cyber topic for FY 2027-2028. This selected topic will become part of the assurance projects selected for inclusion as part of the FY 2027-2028 Annual Audit Plan.

The Office of the Chief Inspector General currently plans to conduct an assurance engagement of the Executive Office of the Governors Appointments Office during FY 2027-2028 and an assurance engagement of the Division of Administration, Human Resources Practices in FY 2028-2029. We further plan to lead and conduct any multi-agency enterprise audit engagements. We further plan to perform our statutorily and professional-standard required responsibilities to include monitoring the status of corrective actions taken on internal audits and to liaison with external auditors as part of their requests to Executive Office of the Governor management.

In addition, the Office of the Chief Inspector General will be continuing our financial emergency monitoring of Local Governmental Entities (LGEs), providing technical assistance to other Offices of Inspector General, managing enterprise priorities for projects as set forth in the General Appropriation Act, and reviewing federal grant monitoring compliance by state agencies.

Long-term audit plans are subject to change based on the results of the periodic risk assessment conducted in accordance with § 20.055, F.S., and requests received from management. The scope of these projects will be determined during the planning phase of these engagements. These plans may also be revised based upon unexpected investigative activity and other requests made by the Governor pursuant to § 14.32(2)(k), F.S.

FINANCIAL EMERGENCY ACTIVITY

Sections 218.50 - 218.504, F.S., make up the state financial emergencies law. The law helps identify and resolve serious financial problems in local government entities before they cause total failure. Under this law, the Executive Office of the Governor serves as the primary enforcement and oversight authority for local governments facing severe financial distress. The Governor has delegated the day-to-day coordination of these tasks to our Office of the Chief Inspector General. Specifically, we determine if state assistance is needed when a local governmental entity meets one or more of the conditions specified in § 218.503(1), F.S.

The Office of the Chief Inspector General collaborates with representatives from the Department of Commerce, Department of Financial Services, Joint Legislative Auditing Committee, Auditor General, Executive Office of the Governor's Office of General Counsel, Office of Policy and Budget, or others as needed in carrying out these responsibilities.



Executive Office of the Governor
Office of the Chief Inspector General
Annual Report FY 2025-2026

City of Opa-Locka

On June 1, 2016, the Governor signed Executive Order #16-135, designating the City of Opa-Locka to be in a state of financial emergency, pursuant to § 218.503, F.S. The City Manager for the City of Opa-Locka had previously requested state financial assistance and the City Commission's June 1, 2016 meeting ratified that request.

The Executive Order created a financial emergency board to oversee the activities of the City of Opa-Locka, designated the Office of the Chief Inspector General as the lead agency in carrying out the Executive Order, and named the Chief Inspector General as the Governor's designee for the City of Opa-Locka to implement measures to resolve the financial emergency.

The Office of the Chief Inspector General performs the following duties as necessary to assist the City of Opa-Locka: review and approve the city budget; evaluate the incurrence of debt; review monthly revenue and expenditures; evaluate financial and contractual obligations; analyze and approve the Five-Year Recovery Plan; review the required audits; review the city's resolutions and ordinances for financial impact; and provide other technical assistance as deemed appropriate.

Local Governmental Entities in Financial Emergency Status

There are approximately 2,445 local governmental entities in Florida.⁹ As of June 30, 2026, no entities were released from financial emergency status and 16 local government entities remain in financial emergency status as defined in § 218.503(3), F.S.¹⁰ These local governmental entities are listed in the following table:

LOCAL GOVERNMENTAL ENTITIES IN FINANCIAL EMERGENCY STATUS
Crossings at Fleming Island Community Development District (CDD)
City of Gretna
City of Pahokee
City of Hampton
City of Opa-Locka
City of Westville
Eastpoint Sewer and Water District

⁹ This includes 67 county governments; 411 incorporated cities, towns, and villages; and approximately 1,967 independent and dependent special districts such as community development and fire control districts.

¹⁰ Please note that all 16 entities currently in a state of financial emergency were determined to be such prior to 2004. Prior to 2004, any local government entity that met a technical condition of a financial emergency, such as deficit fund balance for two successive years, was automatically determined to be in an official state of financial emergency. After 2004, the law was changed to create a formal review process in which the Office of the Chief Inspector General, as delegated by the Governor, must review the specific circumstances of an entity meeting a trigger conditional to determine if state assistance is needed. As such, after 2004, an entity is only officially declared to be in a state of financial emergency if state assistance or oversight is deemed necessary.



Executive Office of the Governor
Office of the Chief Inspector General
Annual Report FY 2025-2026

LOCAL GOVERNMENTAL ENTITIES IN FINANCIAL EMERGENCY STATUS

Hamilton County Development Authority
Heritage Isles CDD
Leon County Educational Facilities Authority
Suwannee Valley Transit Authority
Suwannee Water and Sewer District
Town of Caryville
Town of Eatonville
Town of Noma
Town of Wausau

During FY 2025-2026, the Office of the Chief Inspector General received notices from the Department of Financial Services, the Auditor General, or the local governmental entities regarding any local governmental entity that met one or more of the conditions of financial emergency specified in § 218.503(1), F.S. The Office of the Chief Inspector General requested additional information from 30 entities for use in determining the entities' financial emergency status and none were determined to have been declared in a state of financial emergency requiring state assistance or oversight as defined in § 218.503(3), F.S. The Office of the Chief Inspector General also monitored the financial condition of various local governmental entities based on concerns discovered through Joint Legislative Auditing Committee meetings, news articles, correspondence from citizens, and questions from state and local government officials.

CONCLUSION

We are distinctly honored and privileged to present this report summarizing the Office of the Chief Inspector General's accomplishments for FY 2025-2026.



Executive Office of the Governor
Office of the Chief Inspector General
The Capitol, Suite 1902
Tallahassee, FL 32399-0001

Office: (850) 717-9264
Fax: (850) 921-0817
Whistle-blower's Hotline: 800-543-5353
http://www.flgov.com/inspector_general