



**Office of Inspector General
Annual Report**

September 29, 2020

Ron DeSantis
GOVERNOR



Dane Eagle
EXECUTIVE DIRECTOR

September 29, 2020

Mr. Dane Eagle
The Caldwell Building, Suite 212
107 East Madison Street
Tallahassee, Florida 32399

Ms. Melinda Miguel, Chief Inspector General
Executive Office of the Governor
The Capitol, Suite 1902
Tallahassee, Florida 32399

Dear Director Eagle and CIG Miguel:

I am pleased to submit the Office of Inspector General's Annual Report for Fiscal Year 2019-2020, as required by section 20.055, Florida Statutes.

We remain committed in our work with the Department's management and staff to promote efficiency, accountability and integrity. Thank you for your continued support.

Sincerely,

James E. Landsberg
Inspector General

Florida Department of Economic Opportunity | Caldwell Building | 107 E. Madison Street | Tallahassee, FL 32399
850.245.7105 | www.FloridaJobs.org
www.twitter.com/FLDEO | www.facebook.com/FLDEO

An equal opportunity employer/program. Auxiliary aids and service are available upon request to individuals with disabilities. All voice telephone numbers on this document may be reached by persons using TTY/TTD equipment via the Florida Relay Service at 711.

TABLE OF CONTENTS

HIGHLIGHTS	1
INTRODUCTION	2
Purpose of this Report	
Summary of the Department	
MISSION AND ORGANIZATION OF THE OIG	4
Accreditation	
Organizational Profile	
Professional Certifications	
Professional Affiliations	
INVESTIGATIONS SECTION	7
Summary of Investigative Activity	
Significant Investigative Projects	
AUDIT SECTION	9
Summary of Services	
Work Plan Development	
Significant Audit Projects	
Summary of Internal Audits	
ATTACHMENT I	17
Additional Investigative Activity	
ATTACHMENT II	19
Additional Audit-Related Activity	

HIGHLIGHTS

The Department of Economic Opportunity's Office of Inspector General (OIG) completed the projects below during the 2019-2020 fiscal year.

Investigative Activity

- Responded to over 6,000 citizens seeking assistance;
- Completed eleven inquiries;
- Closed two formal investigations;
- Coordinated the resolution of seventeen complaints with DEO management and with other parties having appropriate jurisdiction

Audit Activity

- Conducted four operational audits and five management reviews resulting in thirty findings and recommendations;
- Performed liaison and coordination activities for eight external audits;
- Coordinated three external engagements with twelve findings and recommendations; and
- Facilitated corrective action for recommendations in prior audits and reviews

Other Activity

- Conducted a Department-wide risk assessment;
- Prepared the annual and long-term audit work plan;
- Provided technical assistance to Department managers as needed; and
- Conducted management-requested reviews to improve efficiencies in program services

INTRODUCTION

Purpose of this Report

Section 20.055, Florida Statutes, requires each Office of Inspector General to prepare an annual report describing its activities during the preceding state fiscal year. This report includes, but is not limited to:

- A description of activities relating to the development, assessment, and validation of performance measures;
- A description of significant deficiencies relating to the administration of programs and operations of the agency disclosed by investigations, audits, reviews, or other activities;
- A description of the recommendations for corrective action made by the inspector general during the reporting period with respect to significant problems, abuses, or deficiencies identified;
- The identification of each significant recommendation described in previous annual reports on which corrective action has not been completed; and
- A summary of each investigation and audit completed during the reporting period.

This document is presented to the Executive Director of the Florida Department of Economic Opportunity and to Florida's Chief Inspector General.

Summary of the Department

Section 20.60, Florida Statutes, states that the mission of the Department of Economic Opportunity is to assist the Governor in working with the Legislature, state agencies, business leaders, and economic development professionals to formulate and implement coherent and consistent policies and strategies designed to promote economic opportunities for all Floridians. The divisions of the Department are as follows:

1. Strategic Business Development
2. Workforce Services
3. Community Development
4. Information Technology
5. Finance and Administration

The Division of Strategic Business Development provides support for attracting out-of-state businesses to Florida, promoting the creation and expansion of Florida businesses, and facilitating the state's economic development partnerships. The primary initiatives and activities of the Division of Strategic Business Development are carried out in the Bureau of Business and Economic Incentives, the Bureau of Compliance and Accountability, the Bureau of Planning and Partnerships, and the Office of Film and Entertainment.

The Division of Workforce Services partners with CareerSource Florida and the state's 24 Local Workforce Development Boards to strengthen Florida's business climate by supporting employers

and helping Floridians gain employment, remain employed, and advance in their careers. The primary initiatives and activities of the Division of Workforce Services are carried out in the Bureaus of Workforce Statistics and Economic Research, One-Stop and Program Support, and Reemployment Assistance.

The Division of Community Development fosters economic development in the state's rural and urban communities through opportunities, assistance, and partnerships with entities such as the Florida Housing Finance Corporation that balance local and state growth management needs. The primary initiatives and activities of the Division are carried out in the Bureaus of Small Cities and Rural Communities, Community Planning and Growth, and Economic Self Sufficiency.

The Division of Information Technology seeks out opportunities where information technology can help support the creation of jobs in Florida's economy. The primary initiatives and activities of the Division are designed to align everything information technology does with DEO needs. The goals of the Division are to eliminate duplicative services, improve the governance model, and leverage third party verifiable sources for efficiency improvements while enhancing accountability and mission integrity.

The Division of Finance and Administration provides support through management of activities related to budget, finance, general services, and human resources. The primary initiatives and activities of the Division are carried out within the Bureaus of Budget Management, Financial Management, Financial Monitoring & Accountability, General Services, and Human Resource Management.

In addition to these divisions, the Department established the Office of Disaster Recovery. This Office supports communities following disasters by addressing long-term recovery needs for housing, infrastructure, economic development, and mitigation needs that remain after other assistance has been exhausted, including federal assistance as well as private insurance. DEO is the governor-designated state authority responsible for administering all U.S. Department of Housing and Urban Development long-term recovery funds awarded to the state.

MISSION AND ORGANIZATION

As stated in section 20.055, Florida Statutes, the role of the OIG is to provide a central point for coordination of, and responsibility for, activities that promote accountability, integrity, and efficiency in the Department.

The OIG has established the following priorities to help ensure success in fulfilling our mission:

- **Sufficiency** – Provide quality audits, investigations, reviews, and other services in accordance with professional standards and, where applicable, federal and state regulations.
- **Timeliness** – Perform audits, audit resolution, investigations, and reviews in a timely manner.
- **Added Value** – Perform activities designed to add value and improve the Department’s operations.
- **Awareness** – Promote awareness regarding OIG roles and responsibilities as well as awareness regarding the duty to report fraud, waste, and abuse.

The primary goal of OIG is to provide independent and objective information in a timely manner to assist the Department’s Executive Director and management team in fulfilling their duties and responsibilities.

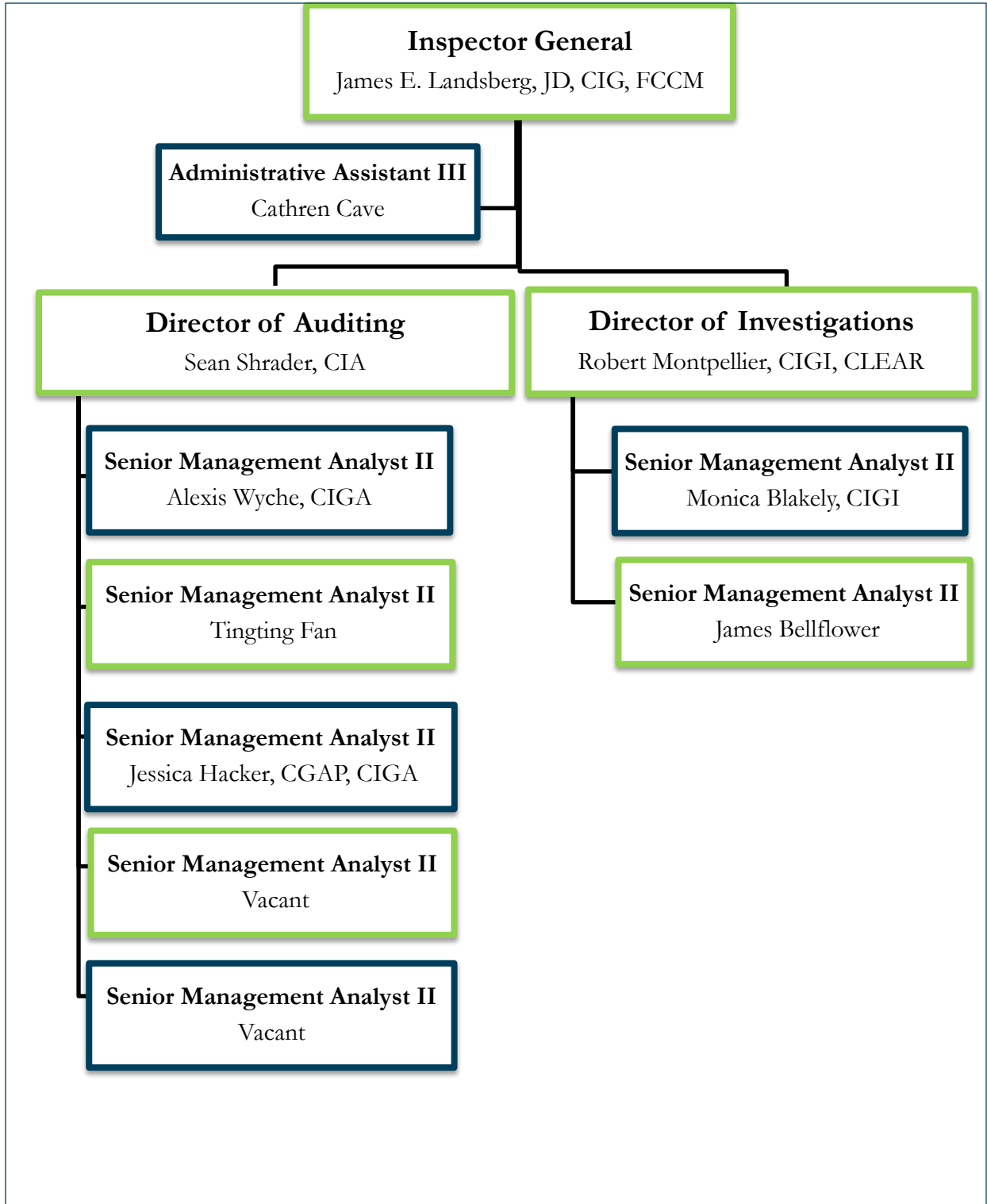
Commission for Florida Law Enforcement Accreditation

As part of OIG’s continuing effort to better accomplish its mission, the Investigations Section pursued credentials through the Commission for Florida Law Enforcement Accreditation. This Commission accredits law enforcement agencies and Offices of Inspectors General within the State of Florida that attain specific standards for operations, investigations, and other activities. The OIG’s Investigations Section achieved reaccreditation on June 26, 2019, after establishing compliance with approximately 40 standards.



Organizational Profile

The OIG had a staff of eleven positions during the fiscal year. Our structure is as follows:



Professional Certifications

Certifications held by the staff include:

- One Certified Inspector General (CIG);
- Two Certified Inspector General Auditors (CIGA);
- One Certified Internal Auditor (CIA);
- Two Certified Inspector General Investigators (CIGI);
- One Certified Government Auditing Professional (CGAP);
- One Certified Investigator/Inspector (CLEAR);
- One Florida Bar Member (JD);
- One Florida Certified Contract Manager (FCCM); and
- One Florida Commission for Law Enforcement Accreditation Certified Assessor

Professional Affiliations

OIG staff members are affiliated with:

- National Association of Inspectors General (AIG);
- Florida Chapter of the Association of Inspector General (FCAIG);
- Institute of Internal Auditors (IIA);
- Tallahassee Chapter IIA (TCIIA);
- The Florida Bar;
- Information Systems Audit and Control Association (ISACA);
- Tallahassee Chapter ISACA (TCISACA);
- Association of Government Accountants (AGA);
- Tallahassee Chapter AGA (TCAGA);
- Council on Licensure, Enforcement, and Regulation (CLEAR); and
- The Florida Commission for Law Enforcement Accreditation

INVESTIGATIONS SECTION

The Investigations Section conducts and coordinates activities designed to detect, deter, and prevent fraud, waste, mismanagement, misconduct, and other abuses. These activities include investigations, inquiries, management referrals, and coordination with law enforcement.

Investigations

The OIG conducts investigations designed to provide Department management with objective, fact-based assessments to help ensure the integrity and efficiency of management and operations. Topics of investigation may include contract procurement violations, conflicts of interest, gross mismanagement, disruptive behavior, falsification of records, and data manipulation. Investigations also encompass misconduct by workforce service providers and other vendors who offer products and services under contract with the Department.

Inquiries

Inquiry cases are opened when it is unclear whether a full investigation is warranted. In these types of cases, fact-gathering is conducted, and a determination is made whether to proceed with a substantive investigation. Inquiries are used to report findings related to complaints or other issues to the Executive Director and Department managers where no specific wrongdoing by any one person is implied. Inquiries concentrate on Department and/or partner processes rather than allegations against a specific subject. An inquiry can result in a written report which summarizes the issues and provides recommendations for correction, if necessary.

Management Reviews

Management Reviews are prompted for a variety of reasons. Primarily, management will request that OIG review a program for inefficiencies or vulnerabilities and make recommendations for improved delivery of programmatic services.

Management Referrals

Management Referral cases are opened when OIG receives complaints which do not rise to the level of significance that warrant a substantive investigation. These complaints are referred to management and are monitored until an outcome report is received and reviewed by OIG.

Law Enforcement Referrals

Law Enforcement Referral cases are those reported to the Florida Department of Law Enforcement (FDLE) or other law enforcement agencies, as appropriate, when the Inspector General has reasonable grounds to believe there has been a violation of criminal law.

Summary of Investigative Activity

The Investigations Section responded to over 6,000 requests for assistance from citizens and completed 30 projects. The table below summarizes significant investigative projects completed during the fiscal year.

Closed Investigative Projects July 1, 2019 – June 30, 2020	
PROJECT	SUMMARY
2019/20-0011	OIG received an anonymous complaint alleging misconduct by DEO employees. OIG investigated and determined the allegation to be unsubstantiated.
2019/20-0024	A complainant alleged that Local Workforce Development Agency (LWDA) staff inaccurately reported their time. OIG conducted an inquiry and determined staff appropriately charged their time to the correct grant. OIG closed this project as there was no law, rule or policy violation.
2019/20-0036	A Reemployment Assistance (RA) claimant alleged that the Director of Workforce Services intentionally delayed processing of her claim and delayed benefit payments. OIG communicated with the complainant and determined that the benefits were properly paid. The complainant had no further concerns.
2019/20-0052	A complainant alleged that an LWDA purchased hazardous, homemade hand sanitizer from the husband of an employee, allowed nepotism in hiring, and allowed employees to take equipment home for their personal use. OIG investigated and found the allegations to be unsubstantiated.
2019/20-0053	A complainant alleged that a grant recipient billed DEO for construction work that was not performed by the grantee's contractor. OIG consulted with the DEO Office of Finance and Accounting and determined that work performed met the criteria of the grant agreement.

**Attachment I includes a summary of additional investigative activity.*

AUDIT SECTION

The Internal Audit function is designed to be an independent, objective assurance and consulting activity which adds value and improves the Department's operations. Its objective is to help the Department accomplish its goals by bringing a systematic, disciplined approach to the evaluation of internal controls and governance processes. Although conducting internal audits is the primary mission of the Audit Section, substantial benefit is provided to the Department through several other functions. These include consulting engagements, coordination with external auditors, resolution of audits with federal grantors, tracking audit findings, and risk analysis.

During Fiscal Year 2019-20, the Internal Audit unit performed four formal audits and five management reviews summarized later in this report. First, we will address the development of our annual and long-term audit work plan.

Work Plan Development

Section 20.055(6)(i), Florida Statutes, requires OIG to develop risk-based annual and long-term audit plans which consider resource requirements and input from senior management.

In March 2020, OIG sent a Risk Assessment Survey to executive management and DEO managers from all divisions and performed in-person interviews with selected senior managers. The risk assessment process had two purposes: (1) To help ensure that Department risk exposures are understood and managed; (2) To assist in identifying OIG work plan assignments. We considered the results of these surveys and interviews in the development of our annual audit plan.

Significant Audit Projects

During fiscal year 2019-20, OIG performed the following tasks related to the development, assessment, and validation of performance measures:

- In June 2020, we assessed the reliability and validity of information provided by the Department for performance measures and standards related to the Long-Range Program Plan (LRPP). In addition, we reviewed the Department's proposed performance measures through FY 2024-25.
- Report No. 2019/20-0042: OIG conducted a review of performance measures reported by the Division of Strategic Business Development (SBD) and contract deliverables reported by Enterprise Florida, Inc. (EFI). This review evaluated the process used to collect, calculate, and report data for selected measures and deliverables. We determined that the SBD measures were valid and reliable, that EFI performance met requirements, and that both SBD and EFI accurately reported relevant data.

Management Reviews

The OIG performed five additional management reviews as part of the audit plan. The findings and recommendations are summarized below.

Management Review of Disaster Recovery Irma Policies and Procedures – Project No. 2019/20-0006

The OIG performed this review as part of the requirement to mitigate fraud, waste and abuse in the disaster recovery program.

We made the following observations:

- The procedures to maintain a comprehensive website did not indicate the frequency of website updates.
- The procedures to enable applicants to determine the status of their applications for recovery assistance, at all phases, did not indicate the frequency of applicant status updates.
- There were no written procedures in place to reprogram funds from stalled projects in a timely manner.
- Although the action plan showed a timeline of how expenditures were projected to be spent within the six-year timeframe, there were no written procedures available to indicate how those projections for the expenditures were made.

We recommended the following:

- Management should update the procedures to indicate the frequency of website updates. At a minimum, the website must be updated monthly.
- Management should update the procedures to indicate the frequency of applicant status updates.
- Management should create and implement written procedures to timely reprogram funds for stalled activities.
- Management should produce written procedures to indicate how projections for expenditures were made.

Management Review of Internal Controls regarding the DAVID System – Project 2019/20-0016

This review is performed annually as part of a contractual requirement between DEO and the Department of Highway Safety and Motor Vehicles to ensure that internal controls are sufficient to protect confidential data.

We made the following observations:

- Some terminated staff continued to have access to DAVID after employment ended, and some current DEO users no longer needed access to complete their assigned duties.

We recommended the following:

- That Workforce Services management (1) ensure supervisors immediately notify the Internal Security Unit (ISU) when subordinates terminate employment or when job duties no longer require access, and (2) timely complete access deactivation forms and submit to the ISU to ensure timely deactivation.

Management Review of Disaster Recovery Hermine/Matthew Policies and Procedures – Project No. 2019/20-0017

The OIG performed this review as part of the requirement to mitigate fraud, waste and abuse in the disaster recovery program.

No recommendations resulted from this review.

Management Review of DEO’s Security Controls for the Florida Department of Highway Safety and Motor Vehicles’ Data Exchange – Project 2019/20-0015

This review is performed annually as part of a contractual requirement between DEO and the Department of Highway Safety and Motor Vehicles to ensure that internal controls are sufficient to protect confidential data.

This review concluded that corrective actions were taken to address prior deficiencies and that internal controls over the data exchange are adequate to protect the confidential data from unauthorized access, distribution, use, modification and disclosure.

Management Review of Florida Housing Performance Measures – Project No. 2018/19-0040

This review was performed on a quarterly basis to ensure that Florida Housing Finance Corporation had appropriately met and reported the results of their quarterly performance measures. Each of the quarterly reports reviewed by OIG correctly reported their performance measures as met.

Audits

The OIG performed five formal audits as part of the audit plan. The findings and recommendations are summarized below.

Audit of Personally Identifiable Information Internal Control Practices at Capital Area Community Action Agency – Project No. 2018/19-0056

This operational audit focused on selected physical and electronic internal controls used by the Capital Area Community Action Agency (CACAA) to protect personally identifiable information (PII) collected during the application process for federal community assistance grants which are administered by the DEO Division of Community Development (DCD). Specifically, we evaluated internal controls in place to protect PII from unintended disclosure.

The OIG made six findings. Additionally, we made two confidential findings that were not placed in the public report but were summarized in finding number six. Specifically, we noted the following:

- CACAA had not established a comprehensive security awareness training program to facilitate all Agency employees' ongoing education and training on security responsibilities and the handling of sensitive and confidential information.
- CACAA did not have a written PII breach response plan that includes policies and procedures for reporting, investigating, managing and documenting a PII data breach.
- CACAA did not timely remove IT access privileges of a user who separated from employment or when the access to the IT resource was no longer needed.
- CACAA did not have a formal process for access authorizations or use access authorization forms for employees to gain access to the Agency's information system.
- Periodic user access reviews did not occur on user accounts that access PII of the client requesting federal funds.
- Certain security controls related to user authentication and transmission of electronic data needed improvement.

We recommended the following:

- That CACAA management establish a comprehensive security awareness training program and ensure that employees timely receive security awareness training and that documentation of the training is maintained to demonstrate compliance with Agency policies.
- That CACAA management review OMB Memorandum 17-12 (Preparing for and Responding to a breach of personally identifiable information) to help develop a written PII breach response plan to ensure a minimum business impact in the event of a major disruption.
- That CACAA management improve procedures to ensure that CMTTools and System user accounts are timely deactivated upon a user's transfer or separation from Agency employment.
- That CACAA management maintain complete and accurate documentation demonstrating management's authorization of CMTTools and network user access privileges.
- That CACAA management establish procedures for, and perform periodic reviews of, information system accounts and associated privileges to ensure that access privileges are authorized and remain appropriate.
- That CACAA management improve IT security controls related to user authentication and data transmission to ensure the confidentiality, integrity and availability of the Agency's data and IT resources.

Management concurred with all six findings (including finding six which consisted of two separate confidential issues) and has completed corrective actions for two of those findings. Corrective action is partially completed for the remaining findings.

Audit of Personally Identifiable Information Internal Control Practices at Suwannee River Economic Council Community Action Agency – Project 2018/19-0078

This operational audit focused on selected physical and electronic internal controls utilized by the Suwannee River Community Action Agency to protect personally identifiable information collected during the application process for federal community assistance grants which are administered by the DEO Division of Community Development. Specifically, we evaluated internal controls in place to protect PII from unintended disclosure.

The OIG made eight findings. Additionally, we made three confidential findings that were not placed in the public report but were summarized in finding number eight.

- Information Technology (IT) resources used to store and transmit confidential data were not inventoried and managed by the Agency.
- Security awareness education was not developed and implemented by the Agency for all employees and contractors.
- Policies and procedures regarding the sanitization of storage media had not been developed and implemented by the Agency.
- Computer access authorizations were not documented or maintained by the Agency.
- The Agency did not conduct periodic reviews of access privileges.
- The Agency did not ensure that IT resources are disabled when they are no longer needed, nor did the Agency established user access disablement time parameters.
- The agency did not have a written incident response plan.
- Security controls related to user identification, password management, and authentication management within the Agency needed improvement.

We recommended the following:

- That management revise its property and equipment policy to ensure that all physical devices and systems within the Agency used to store or transmit data, regardless of acquisition cost, be inventoried and managed.
- That management utilize NIST Special Publication (SP) 800-50: *Building an Information Technology Security Awareness and Training Program*, to develop and implement a security awareness training program for all employees that complies with applicable federal and state rules and regulations.
- The management review NIST Special Publication 800-88: *Guidelines for Media Sanitization*, to ensure the development of a comprehensive media disposal and sanitization procedure that complies with applicable federal and state rules and regulations.
- That management improve controls to ensure that access privileges are only granted based on properly completed and approved access authorization records and require that such records be retained.
- That management ensure that periodic reviews of all user accounts are conducted, and that documentation of such reviews is maintained.
- That management develop and implement a process for the timely deactivation of user accounts upon termination of employment or a change in work duties.

- That management develop and implement a comprehensive incident response plan. At a minimum the plan should include: 1) procedures for capturing and maintaining applicable events; 2) the process for involving appropriate authorities; 3) the process for notifying applicable parties of a security breach; and 4) identification of individuals trained to analyze incidents and the training requirements for those individuals.
- That management improve IT security controls related to user identification, password management, and authenticator management to ensure the confidentiality, integrity and availability of the Agency's data and IT resources.

Management concurred with the above findings and has completed corrective actions to address the issues.

Audit of Personally Identifiable Information Internal Control Practices at Tri-County Community Council – Project 2019/20- 0001

This operational audit focused on selected physical and electronic internal controls utilized by the Tri-County Community Council (TCCC) to protect personally identifiable information collected during the application process for federal community assistance grants which are administered by the DEO Division of Community Development. Specifically, we evaluated internal controls in place to protect PII from unintended disclosure.

The OIG made seven findings. Additionally, we made two confidential findings that were not placed in the public report but were summarized in finding number seven.

- The agency had not established a comprehensive security awareness training program to facilitate all Agency employees' ongoing education and training on security responsibilities and the handling of sensitive and confidential information.
- The Agency did not have a written security incident response plan that includes policies and procedures for reporting, investigating, managing and documenting security incidents such as a breach of PII.
- The Agency did not always comply with State or its own records retention requirements.
- The Agency had not established a formal media disposal process including tracking, securing and sanitizing media to protect sensitive and confidential information contained therein from disclosure.
- The agency did not have a formal process for access authorizations or use access authorization forms for employees to gain access to confidential client PII data.
- Periodic user access reviews did not occur on user accounts that access client PII.
- Certain security controls related to user authentication and storage media protection need improvement.

We recommended the following:

- That management establish a comprehensive security awareness training program and ensure that employees timely receive security awareness training and that documentation of the training is maintained to demonstrate compliance with Agency policies.

- That management review OMB memorandum M-17-12 (Preparing for and responding to a breach of personally identifiable information) to help develop a written incident response plan. At a minimum, the plan should include: 1) procedures for capturing and maintaining applicable events; 2) the process for involving appropriate authorities; 3) the process for notifying applicable parties of a security breach; and 4) identification of individuals trained to analyze incidents and the training requirements for those individuals.
- That management improve its records management program to ensure that all public records, regardless of the format in which they reside, are maintained and disposed of as required by Chapter 119, Florida Statutes.
- That management establish a formal media disposal process including tracking, securing and sanitizing media, addressing the use of appropriate sanitization methods and the safeguarding of media awaiting disposal to ensure accountability and control over media and to protect any confidential and exempt information contained therein.
- That management maintain complete and accurate documentation demonstrating authorization of CMTTools access privileges.
- That management establish procedures for, and perform periodic reviews of, CMTTools accounts and associated privileges to ensure that access privileges are authorized and remain appropriate.
- That management improve IT security controls related to user authentication and storage media encryption to ensure the confidentiality, integrity and availability of the Agency's data and IT resources.

Management concurred with the above findings and has completed corrective actions to address the issues.

Audit of SUNTAX User Access Controls – Project 2019/20-0005

This operational audit focused on information security controls implemented by DEO for managing user access to confidential data maintained within the Department of Revenue (DOR) System for Unified Taxation (SUNTAX).

The OIG made four findings.

- The Division of Workforce Services' Internal Security Unit (ISU) did not retain access authorization forms or confidentiality agreements for all employees given access to SUNTAX.
- The ISU did not timely deactivate SUNTAX privileges after employees' interagency transfers or separation from employment.
- The ISU did not have an adequate process for the periodic review of access privileges to SUNTAX.
- The ISU's written policies and procedures for user access to SUNTAX did not provide the level of security necessary to protect confidential data.

We recommended the following:

- That the ISU improve controls to ensure that access privileges are only granted based on properly completed and approved access authorization records and require that such records be retained.
- That the ISU improve procedures to ensure that access privileges are deactivated in a timely manner when employment is terminated, or duties change to minimize the risk of compromise to DEO's confidential data.
- That the ISU improve procedures for an effective periodic review of access privileges to ensure that those privileges are authorized and remain appropriate.
- That the ISU establish a comprehensive security management program that includes written policies and procedures regarding access controls, disablement of access, and the monitoring of such controls.

Management concurred with the above findings and is planning corrective action to address the issues.

**Attachment II includes a summary of additional audit-related activity.*

ATTACHMENT I

Additional Investigative Activity July 1, 2019 – June 30, 2020	
PROJECT	SUMMARY
2019/20-0002	A business owner alleged that a DOR employee failed to provide requested documents. OIG referred the complainant to DOR OIG for action deemed appropriate.
2019/20-0007	A DEO employee alleged her duties were changed without being compensated. OIG encouraged the complainant to follow the grievance process outlined in the DEO Employee Handbook if not satisfied with her chain of command's response to her concern.
2019/20-0008	A county requested OIG's assistance in determining whether an invoice of a contractor met the criteria for an allowable expense of a grant. OIG determined it was allowable.
2019/20-0009	A former DEO employee complained that she was fired for reporting misfeasance, malfeasance and gross misconduct to her supervisor. OIG attempted to interview the complainant through her attorney and was advised that they were allowing the Florida Commission on Human Relations (FCHR) to conduct the investigation.
2019/20-0010	An employer disputed an RA determination. The employer's issue was sent back to be re-adjudicated. The adjudicator contacted the employer and the claimant to review the separation and make a re-determination.
2019/20-0014	A former LWDA employee alleged that management created a toxic work environment for staff. OIG made the appropriate referrals.
2019/20-0018	A citizen alleged he was the target of a fraudulent check scheme for Community Development Block Grant (CDBG) funds. OIG referred the complaint to local law enforcement.
2019/20-0019	OIG received a complaint alleging discrimination and hostile work environment at a juvenile detention center. OIG referred the complainant to the appropriate agency.
2019/20-0020	An RA claimant expressed concerns about the information he was being asked to submit to authenticate his locked claim. OIG referred his concern to the RA FIRRE unit and the issue was resolved.
2019/20-0022	A complainant alleged he was not paid for wages worked through various day-labor employers. The complainant also requested assistance in obtaining an attorney. OIG made the appropriate referrals.
2019/20-0025	A citizen alleged he was the target of a financial fraud scheme related to CDBG funds. OIG interviewed the complainant and referred the concerns to local law enforcement.
2019/20-0026	A complainant alleged that a CDBG Center Manager inaccurately reported the hours she worked. OIG determined that the applicable contract paid wages based upon monthly deliverables achieved and not by hours.

2019/20-0028	A complainant alleged there was a scam related to CDBG funding. OIG contacted law enforcement and recommended that CDBG post information about identifying scams.
2019/20-0030	An RA claimant alleged that an Appeals Referee was unprofessional and rude to her during her appeals hearing. OIG referred the complaint to the RA Appeals Bureau Chief for review and action deemed appropriate.
2019/20-0032	A complainant alleged that a Strategic Business Development recipient was overbilling for services performed. OIG continues to monitor as other offices review.
2019/20-0034	A TANF recipient filed a complaint regarding her TANF benefits being terminated. OIG contacted the LWDA and the concerns were resolved.
2019/20-0035	An employee in a one-stop career center allegedly made negative comments about a jobseeker with a disability. OIG coordinated with the LWDA and the DEO Office for Civil Rights (OCR). The case was closed due to lack of information from the complainant.
2019/20-0037	OIG received a complaint about an LWDA employee. OIG obtained documents related to the allegations and provided them to management for action deemed appropriate.
2019/20-0038	A jobseeker alleged that an LWDA failed to provide transportation assistance (bus passes) to eligible jobseekers. OIG referred the complaint to One-Stop Program Support.
2019/20-0039	An anonymous complainant alleged that LWDA management treated staff poorly. OCR attempted to conduct an interview but received no response. OIG also forwarded the complaint to the LWDA and received a response.
2019/20-0040	A complainant alleged he was discriminated against by Meals on Wheels. OIG made the appropriate referrals.
2019/20-0044	OIG received an anonymous complaint from Department of State OIG that an individual was receiving RA benefits while working. OIG determined that no RA benefits were being paid to anyone matching the individual's identifying information.
2019/20-0046	An RA claimant alleged that DEO wrongfully withheld a percentage of his RA benefits. The issue involved child support deductions and options were provided to the complainant.
2019/20-0054	An applicant for a Small Business Emergency Bridge Loan alleged she was discriminated against because of her race. OIG referred the complaint to OCR.
2019/20-0064	An RA claimant alleged his account had been hijacked. OIG conducted an inquiry and determined the allegation to be unsubstantiated.

ATTACHMENT II

Additional Audit-Related Activity July 1, 2019 – June 30, 2020	
PROJECT	SUMMARY
2019/20-0003	Coordinated an update of the Catalog of State Financial Assistance.
2019/20-0004	Performed liaison activities related to state and federal audit projects. Specific projects were: <ul style="list-style-type: none">• Auditor General Federal Awards Audit for fiscal year 2018-19• Auditor General Audit of Selected Administrative Controls• OPPAGA Review of Economic Development Program• Six-month follow-up on the Auditor General Reemployment Assistance CONNECT Audit, Report No. 2019-183• Six-month follow-up on the Auditor General Federal Awards Audit for 2018, Report No. 2019-186• Six-month follow-up on the Auditor General Operational audit of Selected Administrative Activities, Report No. 2020-017
2019/20-0012	Performed a consulting review for the Division of Information Technology related to administrator account access.
2019/20-0049	Performed the 2020-21 risk assessment and developed the annual work plan.

— End of Report —

