STATE OF ILLINOIS
OFFICE OF THE
AUDITOR GENERAL
Frank J. Mautino, Auditor General

SUMMARY REPORT DIGEST

OFFICE OF EXECUTIVE INSPECTOR GENERAL FOR AGENCIES OF THE ILLINOIS GOVERNOR

State Compliance Examination
For the Two Years Ended June 30, 2021

Release Date: March 29, 2022

FINDINGS THIS AUDIT: 4			
	New	Repeat	Total
Category 1:	0	0	0
Category 2:	4	0	4
Category 3:	0	0	0
TOTAL	4	0	4
FINDINGS LAST AUDIT: 0			

AGING SCHEDULE OF REPEATED FINDINGS			
Repeated Since	Category 1	Category 2	Category 3
No Repeat Findings			

INTRODUCTION

The Office of Executive Inspector General for the Agencies of the Illinois Governor (Office) was established as an independent State agency charged with investigating allegations of fraud, waste, abuse, mismanagement, misconduct, nonfeasance, misfeasance, malfeasance, and violations of the State Officials and Employees Ethics Act.

SYNOPSIS

- (**21-01**) The Office had not implemented adequate internal controls related to cybersecurity programs, practices and control of confidential information.
- (**21-02**) The Office had not developed a disaster recovery plan.
- (**21-04**) The Office had not implemented adequate internal controls over its service providers.

Category 1: Findings that are **material weaknesses** in internal control and/or a **qualification** on compliance with State laws and regulations (material noncompliance).

Category 2: Findings that are **significant deficiencies** in internal control and **noncompliance** with State laws and regulations.

Category 3: Findings that have **no internal control issues but are in noncompliance** with State laws and regulations.

OFFICE OF EXECUTIVE INSPECTOR GENERAL
FOR THE AGENCIES OF THE ILLINOIS GOVERNOR
STATE COMPLIANCE EXAMINATION
For the Two Years Ended June 30, 2021

EXPENDITURE STATISTICS	2021	2020	2019
Total Expenditures	**$ 7,086,286**	**$ 6,812,063**	**$ 6,716,400**
OPERATIONS TOTAL	$ 7,086,286	$ 6,810,448	$ 6,716,400
% of Total Expenditures	100.0%	100.0%	100.0%
Personal Services	5,126,894	4,932,417	4,813,516
Other Payroll Costs (FICA, Retirement)	701,722	731,377	746,969
All Other Operating Expenditures	1,257,670	1,146,654	1,155,915
PERMANENT IMPROVEMENTS	$ -	$ 1,615	$ -
% of Total Expenditures	0.0%	0.0%	0.0%
Total Receipts	$ 2,367	$ 92	$ 18,960
Average Number of Employees	**69**	**70**	**72**

EXECUTIVE INSPECTOR GENERAL
During Examination Period: Susan M. Haling
Currently: Susan M. Haling

FINDINGS, CONCLUSIONS, AND RECOMMENDATIONS

WEAKNESSES IN CYBERSECURITY PROGRAMS AND PRACTICES

The Office had not implemented adequate internal controls related to cybersecurity programs, practices and control of confidential information.

In order to meet its primary role of "investigating allegations of misconduct and making reports of its findings to affected public agencies and officials," the Office utilized several IT applications which contained confidential and personal information

During our examination of the Office's cybersecurity program, practices, and control of confidential information, we noted the Office had not:

Lack of cybersecurity program

- Developed a formal, comprehensive, adequate and communicated security program (including policies, procedures, and processes as well as clearly defined responsibilities over the security of computer programs and data) to manage and monitor the regulatory, legal, environmental and operation requirements.
- Developed a project management framework to ensure new applications and systems were adequately developed and implemented in accordance with management's expectations.

Risk assessment not conducted

- Developed a risk management methodology, conducted a comprehensive risk assessment, and implemented risk reducing internal controls.
- Established a process to review and ensure security incidents identified by the Department of Innovation and Technology (DoIT) involving the Office's systems or data were fully remediated and related vulnerabilities were assessed.

No process to ensure security incidents and vulnerabilities were assessed and remediated

- Established a data classification methodology for classifying its data to ensure adequate protection of the data. (Finding 1, pages 9-11)

We recommended the Office work with DoIT to obtain a detailed understanding of responsibilities related to cybersecurity controls. Additionally, we recommended the Office:

- Develop a formal, comprehensive, adequate, and communicated security program to manage and monitor the regulatory, legal, environmental and operational requirements.
- Develop a project management framework to ensure new applications are adequately developed and

implemented in accordance with management's expectations.

- Develop a risk management methodology, conduct a comprehensive risk assessment, and implement risk reducing internal controls.
- Establish a process to review and ensure security incidents identified by DoIT involving the Office's systems or data are fully remediated and related vulnerabilities are assessed.
- Develop a data classification methodology.

Office partially agreed with finding

The Office partially agreed with this finding and state the development of these cybersecurity programs and practices is contingent upon the work of the DoIT because DoIT maintains the systems at issue, not the Office. Nonetheless, the Office stated they recognize the importance of developing these programs and practices, and will attempt to work with DoIT to develop them.

Accountant's Comment

In an Accountant's Comment we stated cybersecurity is not only based on 'systems' but the Office's entire security posture. Cybersecurity includes, but is not limited to, developing, maintaining, and communicating security policies and procedures, conducting comprehensive risk assessments to identify risk and implementing mitigating controls.

Further, while we agree DoIT is the Office's Information Technology service provider, the Office is ultimately responsible for the security, integrity, and availability of their systems and data.

DISASTER RECOVERY PLANNING WEAKNESSES

The Office had not developed a disaster recovery plan.

Office had not developed a disaster recovery plan

In order to carry out its mission, the Office utilizes two IT applications: Case Management and Canopy. During our examination, we requested the Office's disaster recovery plan to ensure timely recovery of its applications and data. However, the Office had not developed a disaster recovery plan. (Finding 2, pages 12-13)

We recommended the Office work with the Department of Innovation and Technology (DoIT) to determine responsibilities and assist in developing a disaster recovery plan to ensure the timely recovery of their application and data. Additionally, once developed, we recommended the Office periodically test the disaster recovery plan.

Office partially agreed with finding

The Office partially agreed with this finding and stated the development of a Disaster Recovery plan is contingent upon the work of the DoIT because DoIT maintains the systems.

Nonetheless, the Office stated they will attempt to work with DoIT to develop it.

Accountant's Comment

In an Accountant's Comment we stated although DoIT maintains the environment in which the Office's applications and data reside, the Office has the ultimate responsibility for the recovery of their applications and data. As we recommended, the Office should work with DoIT in the development of disaster recovery plans and annual testing.

LACK OF ADEQUATE CONTROLS OVER THE REVIEW OF INTERNAL CONTROLS FOR SERVICE PROVIDERS

The Office had not implemented adequate internal controls over its service providers.

Office unable to provide documentation demonstrating the service providers population was complete and accurate

The Office provided a listing of service providers however, they did not provide documentation demonstrating the population was complete and accurate.

Due to these conditions, we were unable to conclude the Office's population records were sufficiently precise and detailed under the Professional Standards promulgated by the American Institute of Certified Public Accountants (AT-C § 205.35).

Office had not obtained or documented review of SOC reports

Even given the population limitations noted above, we performed testing over the service providers identified by the Office. During our testing, we noted the Office had not obtained System and Organization Control (SOC) reports or conducted independent internal control reviews of the three (100%) service providers identified by the Office. (Finding 4, pages 16-17)

We recommended the Office strengthen its controls in identifying and documenting all service providers utilized. Further, we recommended the Office obtain SOC reports or conduct independent internal control reviews at least annually. In addition, we recommended the Office:

- Monitor and document the operation of the Complementary User Entity Controls (CUECs) related to the Office's operations.
- Either obtain and review SOC reports for subservice organizations or perform alternative procedures to satisfy itself that the existence of the subservice organization would not impact its internal control environment.
- Document its review of the SOC reports and review all significant issues with subservice organizations to ascertain if a corrective action plan exists and when it will be implemented, any impact to the Office, and any compensating controls.

Office disagreed with finding

The Office disagreed with this rising to the level of a material finding and stated the Office has a limited number of service providers (3) and the primary service provider is the Department of Innovation and Technology (DoIT). The Office also stated they have received and reviewed SOC reports from DoIT and that this finding appears to be focused on the Office's failure to document those SOC reviews.

Accountant's Comment

In an Accountant's Comment we stated although the Office may only utilize three service providers, it is imperative the Office ensure the internal controls of all service providers are adequate and operating effectively. A means of ensuring such, is obtaining, reviewing, and documenting the review of SOC reports.

In their response, the Office stated they had received and reviewed DoIT's SOC reports. At no time during our examination did the Office provide documentation of obtaining and reviewing the DoIT SOC reports. In fact, during a meeting discussing this finding, we informed the Office that DoIT's SOC reports were available on the Office of the Auditor General's website.

OTHER FINDINGS

The remaining finding pertains to Information Technology Access Weaknesses. We will review the Office's progress towards the implementation of our recommendations in our next State compliance examination.

ACCOUNTANT'S OPINION

The accountants conducted a State compliance examination of the Office for the two years ended June 30, 2021, as required by the Illinois State Auditing Act. The accountants stated the Office complied, in all material respects, with the requirements described in the report.

This State compliance examination was conducted by Adelfia LLC.

SIGNED ORIGINAL ON FILE

JANE CLARK
Division Director

This report is transmitted in accordance with Section 3-14 of the Illinois State Auditing Act.

SIGNED ORIGINAL ON FILE

FRANK J. MAUTINO
Auditor General

FJM:JGR