STATE OF ILLINOIS
OFFICE OF COMPTROLLER
FISCAL OFFICER RESPONSIBILITIES

STATE COMPLIANCE EXAMINATION

For the Year Ended June 30, 2023

Performed as Special Assistant Auditors
for the Auditor General, State of Illinois

STATE OF ILLINOIS
OFFICE OF COMPTROLLER
FISCAL OFFICER RESPONSIBILITIES
STATE COMPLIANCE EXAMINATION
For the Year Ended June 30, 2023

TABLE OF CONTENTS

State Compliance Examination Report **Page**

STATE OF ILLINOIS
OFFICE OF COMPTROLLER
FISCAL OFFICER RESPONSIBILITIES
COMPLIANCE EXAMINATION
For the Year Ended June 30, 2023

AGENCY OFFICIALS

Comptroller	Susana A. Mendoza
Assistant Comptroller – Fiscal Policy and Budget	Kevin Schoeben
Assistant Comptroller – Operations Division	
July 1, 2022 – December 31, 2022	Ellen M. Andres
January 1, 2023 – June 30, 2023 (Acting)	Ellen M. Andres
July 1, 2023 – September 14, 2023	Vacant
September 15, 2023 – current	Kathleen Killion
Assistant Comptroller – Chicago Office	Cesar Orozco
Chief Legal Counsel	
July 1, 2022 – July 13, 2023	Debjani Desai
July 14, 2023 – current	Adam Alstott
Chief Internal Auditor	
July 1, 2022 – September 15, 2022	Marvin Becker
September 16, 2022 – current	Teri L. Taylor

AGENCY OFFICES

The Office's primary administrative offices are located at:

Capitol Building
201 State Capitol
Springfield, Illinois 62706-0001

Land of Lincoln Building
325 West Adams Street
Springfield, Illinois 62704-1871

555 West Monroe Street
Suite 1400S-A
Chicago, Illinois 60661-3713

ILLINOIS OFFICE OF COMPTROLLER

SUSANA A. MENDOZA
COMPTROLLER

MANAGEMENT ASSERTION LETTER

January 26, 2024

Sikich LLP
132 South Water Street, Suite 300
Decatur, IL 62523

Dear Sikich:

We are responsible for the identification of, and compliance with, all aspects of laws, regulations, contracts, or grant agreements that could have a material effect on the operations of the State of Illinois, Office of Comptroller – Fiscal Officer Responsibilities (Office). We are responsible for and we have established and maintained an effective system of internal controls over compliance requirements. We have performed an evaluation of the Office's compliance with the following specified requirements during the one-year period ended June 30, 2023. Based on this evaluation, we assert that during the year ended June 30, 2023, the Office has materially complied with the specified requirements listed below.

A. The Office has obligated, expended, received, and used public funds of the State in accordance with the purpose for which such funds have been appropriated or otherwise authorized by law.

B. The Office has obligated, expended, received, and used public funds of the State in accordance with any limitations, restrictions, conditions, or mandatory directions imposed by law upon such obligation, expenditure, receipt, or use.

C. The Office has complied, in all material respects, with applicable laws and regulations, including the State uniform accounting system, in its financial and fiscal operations.

D. State revenues and receipts collected by the Office are in accordance with applicable laws and regulations and the accounting and recordkeeping of such revenues and receipts is fair, accurate, and in accordance with law.

555 West Monroe Street, 1400S-A
Chicago, Illinois 60661-3713
(312) 814-2451

325 West Adams Street
Springfield, Illinois 62704-1871
(800) 877-8078

E. Money or negotiable securities or similar assets handled by the Office on behalf of the State or held in trust by the Office have been properly and legally administered, and the accounting and recordkeeping relating thereto is proper, accurate, and in accordance with law.

Yours truly,

State of Illinois Office of Comptroller – Fiscal Officer Responsibilities

SIGNED ORIGINAL ON FILE

Susana Mendoza, Comptroller

SIGNED ORIGINAL ON FILE

Kathleen Killion, Assistant Comptroller,
Operations Division

SIGNED ORIGINAL ON FILE

Adam Alstott, Chief Legal Counsel

STATE OF ILLINOIS
OFFICE OF COMPTROLLER
FISCAL OFFICER RESPONSIBILITIES
STATE COMPLIANCE EXAMINATION
For the Year Ended June 30, 2023

STATE COMPLIANCE REPORT

SUMMARY

The State compliance testing performed during this examination was conducted in accordance with attestation standards established by the American Institute of Certified Public Accountants; the standards applicable to attestation engagements contained in *Government Auditing Standards* issued by the Comptroller General of the United States; the Illinois State Auditing Act (Act); and the *Audit Guide.*

ACCOUNTANT'S REPORT

The Independent Accountant's Report on State Compliance and on Internal Control Over Compliance does not contain scope limitations or disclaimers but does contain a modified opinion on compliance and identifies material weaknesses over internal control over compliance.

SUMMARY OF FINDINGS

Number of	Current Report	Prior Report
Findings	6	6
Repeated Findings	6	1
Prior Recommendations Implemented or Not Repeated	0	0

SCHEDULE OF FINDINGS

Item No.	Page	Last/First Reported	Description	Finding Type
			Current Findings	
2023-001	9	2022/2009	Late payment of statutorily mandated transfers	Material Noncompliance
2023-002	12	2022/2022	Failure to implement adequate Information Technology controls	Material Weakness and Material Noncompliance
2023-003	15	2022/2022	Inadequate controls over remote access	Significant Deficiency and Noncompliance

Item No.	Page	Last/First Reported	Description	Finding Type
			Current Findings	
2023-004	17	2022/2022	Inadequate disaster recovery planning	Significant Deficiency and Noncompliance
2023-005	19	2022/2022	Weaknesses in cybersecurity programs and practices	Significant Deficiency and Noncompliance
2023-006	21	2022/2022	Inadequate controls over service providers	Material Weakness and Material Noncompliance

EXIT CONFERENCE

The Office waived an exit conference in a correspondence from Teri Taylor, Chief Internal Auditor, on January 17, 2024.

The responses to the recommendations for items 2023-001 and 2023-002 were provided by Ms. Teri Taylor, Chief Internal Auditor, in a correspondence dated December 7, 2023.

The responses to the recommendations for items 2023-003 through 2023-006 were provided by Ms. Teri Taylor, Chief Internal Auditor, in a correspondence dated January 26, 2024.

SIKICH

CERTIFIED PUBLIC ACCOUNTANTS & ADVISORS
Members of American Institute of Certified Public Accountants

132 South Water St., Suite 300
Decatur, IL 62523
217.423.6000

SIKICH.COM

INDEPENDENT ACCOUNTANT'S REPORT ON STATE COMPLIANCE AND ON INTERNAL CONTROL OVER COMPLIANCE

Honorable Frank J. Mautino
Auditor General
State of Illinois

Report on State Compliance

As Special Assistant Auditors for the Auditor General, we have examined compliance by the State of Illinois, Office of Comptroller – Fiscal Officer Responsibilities (Office) with the specified requirements listed below, as more fully described in the *Audit Guide for Financial Audits and Compliance Attestation Engagements of Illinois State Agencies* (*Audit Guide*) as adopted by the Auditor General, during the year ended June 30, 2023. Management of the Office is responsible for compliance with the specified requirements. Our responsibility is to express an opinion on the Office's compliance with the specified requirements based on our examination.

The specified requirements are:

A. The Office has obligated, expended, received, and used public funds of the State in accordance with the purpose for which such funds have been appropriated or otherwise authorized by law.

B. The Office has obligated, expended, received, and used public funds of the State in accordance with any limitations, restrictions, conditions, or mandatory directions imposed by law upon such obligation, expenditures, receipt, or use.

C. The Office has complied, in all material respects, with applicable laws and regulations, including the State uniform accounting system, in its financial and fiscal operations.

D. State revenues and receipts collected by the Office are in accordance with applicable laws and regulations and the accounting and recordkeeping of such revenues and receipts is fair, accurate, and in accordance with law.

E. Money or negotiable securities or similar assets handled by the Office on behalf of the State or held in trust by the Office have been properly and legally administered, and the accounting and recordkeeping relating thereto is proper, accurate, and in accordance with law.

Our examination was conducted in accordance with attestation standards established by the American Institute of Certified Public Accountants, the standards applicable to attestation engagements contained in *Government Auditing Standards* issued by the Comptroller General of the United States, the Illinois State Auditing Act (Act), and the *Audit Guide*. Those standards, the Act, and the *Audit Guide* require that we plan and perform the examination to obtain reasonable assurance about whether the Office complied with the specified requirements in all material respects. An examination involves performing procedures to obtain evidence about whether the Office complied with the specified requirements. The nature, timing, and extent of the procedures selected depend on our judgment, including an assessment of the risks of material noncompliance with the specified requirements, whether due to fraud or error. We believe that the evidence we obtained is sufficient and appropriate to provide a reasonable basis for our modified opinion.

We are required to be independent and to meet our other ethical responsibilities in accordance with relevant ethical requirements relating to the engagement.

Our examination does not provide a legal determination on the Office's compliance with the specified requirements.

Our examination disclosed material noncompliance with the following specified requirements applicable to the Office during the year ended June 30, 2023. As described in the accompanying Schedule of Findings as item 2023-001, the Office had not obligated, expended, received, and used public funds of the State in accordance with any limitations, restrictions, conditions, or mandatory directions imposed by law upon such obligation, expenditure, receipt, or use. Additionally, as described in the accompanying Schedule of Findings as items 2023-002 and 2023-006, the Office had not complied, in all material respects, with applicable laws and regulations.

In our opinion, except for the material noncompliance with the specified requirements described in the preceding paragraph, the Office complied with the specified requirements during the year ended June 30, 2023, in all material respects. However, the results of our procedures disclosed instances of noncompliance with the specified requirements, which are required to be reported in accordance with criteria established by the *Audit Guide* and are described in the accompanying Schedule of Findings as items 2023-003 through 2023-005.

The Office's responses to the compliance findings identified in our examination are described in the accompanying Schedule of Findings. The Office's responses were not subjected to the procedures applied in the examination and, accordingly, we express no opinion on the responses.

The purpose of this report is solely to describe the scope of our testing and the results of that testing in accordance with the requirements of the *Audit Guide*. Accordingly, this report is not suitable for any other purpose.

Report on Internal Control Over Compliance

Management of the Office is responsible for establishing and maintaining effective internal control over compliance with the specified requirements (internal control). In planning and performing our examination, we considered the Office's internal control to determine the examination procedures that are appropriate in the circumstances for the purpose of expressing our opinion on the Office's compliance with the specified requirements and to test and report on the Office's

internal control in accordance with the *Audit Guide*, but not for the purpose of expressing an opinion on the effectiveness of the Office's internal control. Accordingly, we do not express an opinion on the effectiveness of the Office's internal control.

Our consideration of internal control was for the limited purpose described in the preceding paragraph and was not designed to identify all deficiencies in internal control that might be material weaknesses or significant deficiencies and, therefore, material weaknesses or significant deficiencies may exist that have not been identified. However, as described in the accompanying Schedule of Findings, we did identify certain deficiencies in internal control that we consider to be a material weakness and significant deficiencies.

A deficiency in internal control exists when the design or operation of a control does not allow management or employees, in the normal course of performing their assigned functions, to prevent, or detect and correct, noncompliance with the specified requirements on a timely basis. A material weakness in internal control is a deficiency, or a combination of deficiencies, in internal control, such that there is a reasonable possibility that a material noncompliance with the specified requirements will not be prevented, or detected and corrected, on a timely basis. We consider the deficiencies described in the accompanying Schedule of Findings as items 2023-002 and 2023-006 to be material weaknesses.

A significant deficiency in internal control is a deficiency, or a combination of deficiencies, in internal control that is less severe than a material weakness, yet important enough to merit attention by those charged with governance. We consider the deficiencies described in the accompanying Schedule of Findings as items 2023-003 through 2023-005 to be significant deficiencies.

As required by the *Audit Guide*, immaterial findings excluded from this report have been reported in a separate letter.

The Office's responses to the internal control findings identified in our examination are described in the accompanying Schedule of Findings. The Office's responses were not subjected to the procedures applied in the examination and, accordingly, we express no opinion on the responses.

The purpose of this report is solely to describe the scope of our testing of internal control and the results of that testing based on the requirements of the *Audit Guide*. Accordingly, this report is not suitable for any other purpose.

SIGNED ORIGINAL ON FILE

Decatur, Illinois
January 26, 2024

STATE OF ILLINOIS
OFFICE OF COMPTROLLER
FISCAL OFFICER RESPONSIBILITIES
SCHEDULE OF FINDINGS – CURRENT FINDINGS
Year Ended June 30, 2023

2023-001. **FINDING** (Late payment of statutorily mandated transfers)

The Office of Comptroller (Office) did not ensure all statutorily mandated transfers between State funds were made within established timeframes, as required.

The Office had a system in place to identify and record inter-fund transfers it was required to make. During the fiscal year ended June 30, 2023, the Office timely recorded, within the Statewide Accounting Management System (SAMS), the receivables and related payables for transfers of money in the State Treasury to be made between State of Illinois' funds. However, not all transfers were timely made. During fiscal year 2023, we noted 264 transfers between State funds made greater than 30 days after the statutorily mandated transfer date. Transfers made between one and 30 days after the statutorily mandated transfer date were excluded from the information provided in the following table. The following summary concerning late payment of statutorily mandated transfers highlights the delays of making such transfers in fiscal year 2023 compared to fiscal year 2022:

	Fiscal Year 2023*	**Fiscal Year 2022****
Number of late transfers	264 transfers (127 from General Revenue Fund (GRF))	320 transfers (165 from GRF)
Range of days transfers were late	31 to 299 days	31 to 365 days
Total volume of late transfers, in $	$1.23 billion ($327.98 million from GRF)	$1.25 billion ($332.52 million from GRF)
Late transfers outstanding and paid after June 30	$954.86 million ($0 from GRF)	$876.84 million ($49.69 million from GRF)

**Analysis prepared as of October 30, 2023, for fiscal year 2023.*

***Denotes information from the prior year finding.*

Also, during fiscal year 2023, we noted 182 late transfers, totaling $862.45 million, between State funds made between one and 30 days after the statutorily mandated transfer date.

Furthermore, the following table contains the number of late transfers still outstanding as of October 30, 2023, relating to fiscal years 2023 and 2022.

	Fiscal Year 2023	Fiscal Year 2022
Number of late transfers outstanding as of 10/30/2023	63	21
Amount of late transfers outstanding as of 10/30/2023	$391.43 million	$133.79 million

The transfers noted above are mandated by various State statutes that contain the required funds, amounts, and timeline. This finding was first reported during the fiscal year 2009 financial audit.

Office management stated, as they did during prior examinations, due to continued fiscal circumstances outside the control of the Office, the Office must continue to engage in cash management strategies maximizing the use of State funds while also managing resources on-hand to address various pending vouchers causing some transfers to remain in the SAMS queue until the Office is able to process them.

Office management further stated although it has significantly decreased the payment cycle and the number of late payments by managing revenues on-hand, some transfers cannot be made timely since payments for core State programs are prioritized. Office management also stated the Office policy was to prioritize State obligations for payrolls, pension contributions, human and social services programs, education, and debt service rather than to transfer revenues into funds that have no current demand or funding pressures.

Failure to make inter-fund transfers within applicable timeframes represents noncompliance with State law, and untimely transfers of monies may have delayed the receiving fund's use of appropriated funds. (Finding Code No. 2023-001, 2022-001, 2021-001, 2020-001, 2019-001, 2018-001, 2017-001, 2016-001, 2015-001, 2014-001, 2013-001, 12-1, 11-1, 10-1, 09-1)

RECOMMENDATION

We recommend the Office make transfers within timeframes established by applicable statutes. While we realize the lack of available funds in the State Treasury requires prioritization and cash management decisions, we recommend the Office continue in its efforts to make transfers in as timely a manner as possible.

OFFICE RESPONSE

The Office accepts the recommendation and will continue in its effort to make the required transfers timely but given all the competing payments from limited resources in the State Treasury there will always be some transfers pending until funds are available, or when needed. It should be noted that most GRF transfers were made by the end of June 30, 2023

and the few pending GRF transfers were not delayed. Pending non-GRF transfers, especially those for capital obligations, will be processed upon collaboration with the respective state agencies. The Office staff continues to work together with various State fiscal officers on a regular ongoing basis to manage the processing of such transfers throughout the fiscal year to avoid disruptions in the delivery of State services or programs.

2023-002. **FINDING** (Failure to implement adequate Information Technology controls)

The Office of Comptroller (Office) failed to implement adequate general Information Technology (IT) controls related to its environment and applications.

In order to fulfill its mission as the Comptroller of the State of Illinois, the Office maintains an information technology environment to host its applications and data. To ensure the internal controls over the environment and applications were appropriate, we reviewed the Office's general IT controls: security of the environment, controls over access provisioning and controls over changes. Our testing noted:

Security of the environment
The Office was unable to provide certain requested information covering the audit period concerning the network and related security policies and procedures. In addition, during our review of the documentation that was provided, we noted instances where the network and mainframe environments security settings were not current or properly configured.

Further, we noted instances where the level of administrative access did not appear to be appropriate.

Controls over access provisioning
During our testing of the Office's controls over access provisioning, we noted the Office:

- Had not established policies and procedures documenting requirements for reviewing security reports for the network or all applications.
- Had not established policies and procedures documenting the process for terminating external users' access.
- Did not document its review of mainframe security violation reports.
- Did not conduct timely reviews of the network and mainframe environments security violation reports.
- Did not conduct security logging for all applications.
- Did not document approval for users' access to applications.
- Did not timely terminate separated users' access or have a designated timeframe for which access was to be revoked.
- Did not provide documentation demonstrating separated users' access had been revoked.
- Did not conduct a periodic review of users' access to the network and mainframe environment and applications.

Controls over changes
Our review of the Office's System Development Methodology, System Request Procedures, and Network Change Authorization Form Procedures, and System Administration Guide noted they were not current and did not reflect the Office's process for change management.

We requested the Office's population of changes to the network environment. However, the Office was unable to provide a complete and accurate population of changes, as the Office

did not require all changes to follow the change management process. Therefore, we were unable to test the controls over changes to the network environment.

Additionally, we noted an individual can request and approve, without further approval.

We tested a sample of application changes, noting:

- Documentation was not maintained of the migration dates,
- Systems requests were missing documentation of the requestor and required approvals, and
- Post Implementation Reviews were not completed.

Further, in order to determine whether the Office maintained proper segregation of duties over application changes, we requested the population of developers. In response to our request, the Office provided numerous populations; however, the Office did not provide documentation demonstrating the populations were 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 (AU-C § 500.08).

Even given the population limitations noted above, we tested a sample of application changes to ensure proper segregation of duties. However, the Office did not provide sufficient documentation to determine who conducted the migration. We also noted developers had access to the production environment.

The *Security and Privacy Controls for Information Systems and Organizations* (Special Publication 800-53, Fifth Revision) published by the National Institute of Standards and Technology (NIST), Access Control, Configuration, and the System Development Life Cycle sections, require entities to maintain proper internal controls over the security of the environments, access provisioning and change management.

Also, the Fiscal Control and Internal Auditing Act (30 ILCS 10/3001) requires all State agencies to establish and maintain a system, or systems, of internal fiscal and administrative controls to provide assurance funds, property, and other assets and resources are safeguarded against waste, loss, unauthorized use and misappropriation and maintain accountability over the State's resources.

Further, the Office's Security Administration Guide (Guide) requires the users' supervisor to provide approvals for access. In addition, the Office is to periodically review users' access.

Office management indicated that the items causing auditors to cite concerns were due to incomplete written documentation although technical controls remain in place. However, auditors believe the issues were more than incomplete documentation and also believe the technical controls in place did not address all of the noted concerns. The Office's inability to implement adequate general IT controls was the result of staffing shortages and limited resources.

Inadequate controls over the Office's environment and applications could lead to unauthorized access, unauthorized changes and security risks to its environments, applications and related data. Also, due to the severity of the weaknesses noted, we were unable to rely upon the general IT control over the environments and applications. (Finding Code No. 2023-002, 2022-002)

RECOMMENDATION

We recommend the Office implement adequate general IT controls related to its environments and applications.

OFFICE RESPONSE

The Office accepts the recommendation. The Office must be agile in its operations to ensure statutory requirements are met and adapt when conditions change. The Office will continue to work to update procedures in a timely manner and ensure the required supporting documentation is maintained in accordance with the documented procedures in place, as necessary.

2023-003. **FINDING** (Inadequate controls over remote access)

The Office of Comptroller (Office) did not maintain adequate controls over remote access to its environment, applications, and data.

To enable staff to work from home, the Office allowed staff remote access to its environment, applications, and data. Our review of the Office's controls over remote access noted the Office had not:

- Established policies and procedures to control remote access.
- Communicated requirements to users.
- Periodically reviewed users' remote access.
- Conducted monitoring of remote access.
- Maintained sufficient documentation demonstrating the security controls over remote access.

The *Security and Privacy Controls for Information Systems and Organizations* (Special Publication 800-53, Fifth Revision) published by the National Institute of Standards and Technology (NIST), Access Control and System and Communication Protection sections, requires entities to implement adequate internal controls over access to its environment, applications and data.

The Fiscal Control and Internal Auditing Act (30 ILCS 10/3001) requires all State agencies to establish and maintain a system, or systems, of internal fiscal and administrative controls to provide assurance funds, property and other assets and resources are safeguarded against waste, loss, unauthorized use, and misappropriation and maintain accountability over the State's resources.

Office management indicated that the weaknesses noted above were a result of competing priorities for which their attention was directed.

Without adequate controls over remote access, unauthorized individuals may have access to the environment, applications and data maintained by the Office, which may also result in malicious activity. (Finding Code No. 2023-003, 2022-003)

RECOMMENDATION

We recommend the Office implement controls to ensure the security over remote access to its environment, applications, and data. Specifically, we recommend the Office:

- Establish policies and procedures to control remote access.
- Communicate requirements to users.
- Periodically review users' remote access.
- Monitor remote access.
- Maintain documentation demonstrating the security controls over remote access.

OFFICE RESPONSE

The Office accepts the recommendation. The Office will update the remote access user agreements to communicate user responsibilities and is documenting the technical controls. The Office will formally document the process currently in place for assignment and approval of remote access and establish a process for periodic access reviews.

2023-004. **FINDING** (Inadequate disaster recovery planning)

The Office of Comptroller (Office) did not ensure adequate recovery plans were maintained.

The Office was established to maintain the State's central fiscal accounts, order payments into the treasury and issue warrants against any funds held by the Treasurer. In order to meet its mission, the Office utilizes a myriad of applications.

During our review of the Office's Data Center Contingency Plan (Plan), dated June 28, 2023, we noted the Plan:

- Did not contain or reference detailed recovery scripts for all applications, and
- Did not document the recovery time objective at the application level.

In addition, we noted the Office did not conduct a business impact analysis until June 2023, and the business impact analysis did not contain documentation of management's review.

Further, the recovery testing documentation did not document the recovery of the network or applications and did not provide sufficient details to determine if testing was successful or if errors were encountered.

The *Contingency Planning Guide for Information Technology Systems* published by the National Institute of Standards and Technology (NIST) requires entities to have an updated and regularly tested disaster contingency plan to ensure the timely recovery of applications and data. In addition, a business impact analysis is a key step in implementing contingency planning controls and processes.

The Fiscal Control and Internal Auditing Act (30 ILCS 10/3001) requires all State agencies to establish and maintain a system, or systems, of internal fiscal and administrative controls to provide assurance funds, property and other assets and resources are safeguarded against waste, loss, unauthorized use and misappropriation and maintain accountability over the State's resources.

Office management indicated there were updates made to the Plan during the year. However, due to current procedure design the items noted above were not addressed.

Inadequate recovery plans could result in delayed recovery of the Office's operations and affect the Office's ability to fulfill its mission. (Finding Code No. 2023-004, 2022-004)

RECOMMENDATION

We recommend the Office update the Data Center Contingency Plan to document, or make reference to:

- Detailed recovery scripts for all applications, and
- The recovery time objective at the application level.

Additionally, we recommend the Office's management approve the business impact analysis and review the Data Center Contingency Plan to determine if changes are warranted based on the outcome of the business impact analysis.

Further, we recommend the Office document the errors and success of the recovery testing.

OFFICE RESPONSE

The Office accepts the recommendation. Recovery testing for critical applications is completed annually and if any issues are identified they are addressed accordingly. The Office will make updates to the Data Center Contingency Plan, as needed, to ensure the backup and recovery of the network and applications.

2023-005. **FINDING** (Weaknesses in cybersecurity programs and practices)

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

The Office utilizes various applications which contain a significant amount of critical and confidential data, such as names, addresses, Social Security numbers, banking information, etc.

The Illinois State Auditing Act (30 ILCS 5/3-2.4) requires the Auditor General to review State agencies and their cybersecurity programs and practices. During our examination of the Office's cybersecurity programs, practices and control of confidential information, we noted the Office had not:

- Developed policies and procedures related to:
  - Configuration management,
  - Access control for all environments, and
  - Data loss prevention.
- Established a schedule to review and update security policies and procedures.
- Established a data classification methodology or classified its data most susceptible to attack to ensure adequate protection.
- Developed a risk management methodology and implemented risk reducing internal controls related to the risk identified in the Office's risk assessment.
- Ensured all employees and contractors had completed Cybersecurity Awareness Training.
- Established a project management framework.

Additionally, the Office did not provide a complete population of vulnerability scans or provide documentation of actions taken to ensure ignored or disabled vulnerabilities were being properly protected from exploitation.

The *Framework for Improving Critical Infrastructure Cybersecurity* and the *Security and Privacy Controls for Information Systems and Organizations* (Special Publication 800-53, Fifth Revision) published by the National Institute of Standards and Technology (NIST) requires entities to consider risk management practices, threat environments, legal and regulatory requirements, mission objectives and constraints in order to ensure the security of their applications, data and continued business mission.

The Fiscal Control and Internal Auditing Act (30 ILCS 10/3001) requires all State agencies to establish and maintain a system, or systems, of internal fiscal and administrative controls to provide assurance funds, property and other assets and resources are safeguarded against waste, loss, unauthorized use, and misappropriation and maintain accountability over the State's resources.

Office management indicated the Written Information Security Program which documents cybersecurity policies was not completed due to competing priorities. Management also indicated vulnerability scan documentation had been purged, and therefore the Office was unable to provide all items requested in the sample.

The lack of an adequate cybersecurity program and adequate cybersecurity practices could result in unidentified risks and vulnerabilities, which could ultimately lead to the Office's confidential and personal information being susceptible to cyberattacks and unauthorized disclosure. (Finding Code No. 2023-005, 2022-005)

RECOMMENDATION

We recommend the Office:

- Develop policies and procedures related to:
  - Configuration management,
  - Access control for all environments, and
  - Data loss prevention.
- Establish a schedule to review and update security policies and procedures.
- Establish a data classification methodology or classified its data most susceptible to attack to ensure adequate protection.
- Develop a risk management methodology and implemented risk reducing internal controls related to the risk identified in the Office's risk assessment.
- Ensure all employees and contractors have completed Cybersecurity Awareness Training.
- Establish a project management framework.

Additionally, we recommend the Office ensure documentation of vulnerability scans are maintained including those actions taken to ensure ignored/disabled vulnerabilities are properly protected from exploitation.

OFFICE RESPONSE

The Office accepts the recommendation. The Office will continue its effort to develop the Written Information Security Program to address the items noted above. In addition, the requirement to complete cybersecurity training annually will be added to the employee handbook. The Office is developing a procedure for maintaining documentation on vulnerability scans and actions taken during the fiscal year.

2023-006. **FINDING** (Inadequate controls over service providers)

The Office of Comptroller (Office) had not implemented adequate controls over its service providers.

We requested the Office's population of service providers utilized during the examination period to determine if the Office had reviewed the internal controls of its service providers. In response to our request, the Office provided a population; however, the population contained several inaccuracies and missing information. 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 § 205.36). Therefore, we were unable to conduct detailed testing of the Office's controls over its service providers.

The *Security and Privacy Controls for Information Systems and Organizations* (Special Publication 800-53, Fifth Revision) published by the National Institute of Standards and Technology (NIST), Maintenance and System and Service Acquisition sections, requires entities outsourcing their information technology environment or operations to obtain assurance over the entities' internal controls related to the services provided. Such assurance may be obtained via System and Organization Control reports or independent reviews.

Also, the Fiscal Control and Internal Auditing Act (30 ILCS 10/3001) requires all State agencies to establish and maintain a system, or systems, of internal fiscal and administrative controls to provide assurance funds, property, and other assets and resources are safeguarded against waste, loss, unauthorized use, and misappropriation and maintain accountability over the State's resources.

In the prior year examination, Office management indicated service provider procedures were not formalized due to oversight. During the current examination, Office management indicated it had not completed processes and procedures as a result of competing priorities.

Without having obtained and reviewed SOC reports or another form of independent internal control review, the Office does not have assurance the service providers' internal controls are adequate and operating effectively. (Finding Code No. 2023-006, 2022-006)

RECOMMENDATION

We recommend the Office develop a process to determine their services providers and ensure the controls over the service providers are properly reviewed.

OFFICE RESPONSE

The Office accepts the recommendation. The Office is developing a process and formalizing procedures to identify, obtain, and document review of service organizations.