State of Illinois
LEGISLATIVE INFORMATION SYSTEM
STATE COMPLIANCE EXAMINATION
For the Two Years Ended June 30, 2024

STATE OF ILLINOIS
LEGISLATIVE INFORMATION SYSTEM
STATE COMPLIANCE EXAMINATION
For the Two Years Ended June 30, 2024

TABLE OF CONTENTS

STATE OF ILLINOIS
LEGISLATIVE INFORMATION SYSTEM
STATE COMPLIANCE EXAMINATION
For the Two Years Ended June 30, 2024

AGENCY OFFICIALS

Executive Director	Mr. Jarred Sampson
Application Services Manager	Mr. Jacob Sampson
Systems Manager	Mr. Dan Winchester (7/1/2022 - 12/31/2024) Mr. Kevin Fry (1/1/2025 - Present)
Administrative Services Manager	Ms. Susan D. Hall
Support Services Manager	Ms. Emily Deakin-Harmony

GOVERNING BOARD MEMBERS

Board Member (Chairperson 10/01/24 – Present)	Mr. Brad Bolin, Assistant Clerk of the House
Board Member (Chairperson 10/01/21 – 09/30/22)	Mr. Scott Kaiser, Assistant Secretary of the Senate
Board Member (Chairperson 10/01/22 – 09/30/23)	Mr. Tim Anderson, Secretary of the Senate
Board Member (Chairperson 10/01/23 – 09/30/24)	Mr. John Hollman, Clerk of the House

Note: The Legislative Commission Reorganization Act of 1984 (Act) (25 ILCS 130/1-5(b)) requires the Board to consist of the Secretary and Assistant Secretary of the Senate and the Clerk and Assistant Clerk of the House of Representatives. Further, the Act requires the Chairperson of the Board to be the member who is affiliated with the same caucus as the then serving Chairperson of the Joint Committee on Legislative Support Services. The Chairperson of the Joint Committee on Legislative Support Services rotates caucuses annually on October 1, therefore, resulting in an annual rotation of Board Chairperson. The Legislative Information System Governing Board shall continue to consist of the four members with the annual rotation of Chairperson.

AGENCY OFFICE

The System's office is located at:

705 Stratton Office Building
Springfield, Illinois 62706

705 Stratton Office Building • Springfield, IL 62706
217 782 3944 TEL • 217 524 6059 FAX

Legislative Information System

MANAGEMENT ASSERTION LETTER

June 17, 2025

Honorable Frank J. Mautino
Auditor General
State of Illinois
400 West Monroe, Suite 306
Springfield, Illinois 62704

Auditor General Mautino:

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, Legislative Information System (System). 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 System's compliance with the following specified requirements during the two-year period ended June 30, 2024. Based on this evaluation, we assert that during the years ended June 30, 2023, and June 30, 2024, the System has materially complied with the specified requirements listed below.

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

Yours truly,

State of Illinois, Legislative Information System

SIGNED ORIGINAL ON FILE

Jarred Sampson, Executive Director

SIGNED ORIGINAL ON FILE

Susan D. Hall, Administrative Services Manager

STATE OF ILLINOIS
LEGISLATIVE INFORMATION SYSTEM
STATE COMPLIANCE EXAMINATION
For the Two Years Ended June 30, 2024

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, disclaimers, or other significant non-standard language.

SUMMARY OF FINDINGS

Number of	**Current Report**	**Prior Report**
Findings	4	3
Repeated Findings	0	0
Prior Recommendations Implemented or Not Repeated	3	2

SCHEDULE OF FINDINGS

Item No.	Page	Last/First Reported	Description	Finding Type
			Current Findings	
2024-001	8	New	Weaknesses in Cybersecurity Programs and Practices	Significant Deficiency and Noncompliance
2024-002	10	New	Weaknesses in Disaster Recovery Planning	Significant Deficiency and Noncompliance
2024-003	12	New	Weaknesses in Change Control Processes	Significant Deficiency and Noncompliance
2024-004	14	New	Weaknesses in Controls over System Security	Significant Deficiency and Noncompliance

SCHEDULE OF FINDINGS

Item No.	Page	Last/First Reported	Description	Finding Type
			Prior Findings Not Repeated	
A	16	2022/2022	Inadequate Controls over Personal Services	
B	16	2022/2022	Inadequate Internal Controls over Census Data	
C	16	2022/2022	Inadequate Controls over Reconciliations	

EXIT CONFERENCE

The System waived an exit conference in a correspondence from Susan Hall, Administrative Services Manager, on June 17, 2025. The responses to the recommendations were provided by Susan Hall, Administrative Services Manager, in a correspondence dated June 17, 2025.

SPRINGFIELD OFFICE:
400 WEST MONROE
SUITE 306 • 62704
PHONE: 217/782-6046 • FAX: 217/785-8222
TTY: 888/261-2887
FRAUD HOTLINE: 1-855-217-1895

CHICAGO OFFICE:
MICHAEL A. BILANDIC BLDG. • SUITE S-900
160 NORTH LASALLE • 60601-3103
PHONE: 312/814-4000
FAX: 312/814-4006
FRAUD HOTLINE: 1-855-217-1895

OFFICE OF THE AUDITOR GENERAL
FRANK J. MAUTINO

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

We have examined compliance by the State of Illinois, Legislative Information System (System) 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 two years ended June 30, 2024. Management of the System is responsible for compliance with the specified requirements. Our responsibility is to express an opinion on the System's compliance with the specified requirements based on our examination.

The specified requirements are:

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

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 System complied with the specified requirements in all material respects. An examination involves performing procedures to obtain evidence about whether the System complied with the specified requirements. The nature, timing,

E-MAIL ADDRESS: AUDGEN@AUDITOR.ILLINOIS.GOV

and extent of the procedures selected depend on our judgement, 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 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 System's compliance with the specified requirements.

In our opinion, the System complied with the specified requirements during the two years ended June 30, 2024, 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 2024-001 through 2024-004.

The System's responses to the compliance findings identified in our examination are described in the accompanying Schedule of Findings. The System'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 System 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 System's internal control to determine the examination procedures that are appropriate in the circumstances for the purpose of expressing our opinion on the System's compliance with the specified requirements and to test and report on the System's internal control in accordance with the *Audit Guide*, but not for the purpose of expressing an opinion on the effectiveness of the System's internal control. Accordingly, we do not express an opinion on the effectiveness of the System's internal control.

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 material noncompliance with the specified requirements will not be prevented, or detected and corrected, on a timely basis. 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.

Our consideration of internal control was for the limited purpose described in the first paragraph of this section 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. We did not identify any deficiencies in internal control that we consider to be material weaknesses. However, we did identify certain deficiencies in internal control, described in the accompanying Schedule of Findings as items 2024-001 through 2024-004 that we consider to be significant deficiencies.

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

The System's responses to the internal control findings identified in our examination are described in the accompanying Schedule of Findings. The System'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

COURTNEY DZIERWA, CPA, CISA, CIA
Director of Financial and Compliance Audits

Springfield, Illinois
June 17, 2025

2024-001. **FINDING** (Weaknesses in Cybersecurity Programs and Practices)

The Legislative Information System (System) had not implemented adequate internal controls related to cybersecurity programs and practices.

The System carries out its mission through the use of Information Technology (IT), including various applications, which contains confidential or personal information such as names, addresses, and Social Security numbers.

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 System's cybersecurity programs, practices, and control of confidential information, we noted the System had not:

- Maintained a configuration management policy outlining the controls over device configurations, including baseline configurations.
- Maintained policies and procedures requiring staff to report suspected security violations and events.
- Maintained adequate documentation demonstrating the annual review and revision of policies and procedures.
- Maintained a detailed risk management methodology addressing categorization of information systems, authorization of information system access, and monitoring security controls.
- Maintained a data classification methodology or classified its data most susceptible to attack to ensure adequate protection.
- Communicated cybersecurity or security related policies to staff to acknowledge their understanding of responsibilities.
- Maintained policies and procedures for data retention and access permissions for confidential information.
- Utilized a login banner on the System network to warn against unauthorized access.
- Maintained documentation of vulnerability scans conducted and corrective actions taken demonstrating the System monitored and responded timely to network threats.

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 (AC-1, AC-2, AC-3, AC-8), Configuration Management (CM-1), System and Services Acquisition, Risk Assessment (RA-2, RA-5), Incident Response (IR-1, IR-2), and Awareness and Training (AT-1, AT-2) sections, 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.

2024-001. **FINDING** (Weaknesses in Cybersecurity Programs and Practices) – Continued

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 to maintain accountability over the State's resources.

System officials stated historical reliance on informal or ad-hoc documentation processes, combined with limited dedicated resources for formalizing detailed policy documentation and employee training acknowledgment, contributed to the identified gaps.

The lack of adequate cybersecurity programs and practices could result in unidentified risks and vulnerabilities, which could ultimately lead to the System's confidential and personal information being susceptible to cyberattacks and unauthorized disclosure. (Finding Code No. 2024-001)

RECOMMENDATION

We recommend the System:

- Develop policies and procedures pertaining to:
  - configuration management,
  - reporting security violations and events, and
  - data retention and access permissions for confidential data.
- Establish a schedule to review and update security policies and procedures.
- Develop a detailed risk management methodology.
- Establish a data classification methodology and classify its data most susceptible to attack to ensure adequate protection.
- Communicate cybersecurity or security related policies to staff.
- Establish a login banner for networks prohibiting unauthorized access.
- Maintain supporting documentation of vulnerability scans conducted and corrective actions taken.

SYSTEM RESPONSE

The System accepts the recommendation.

2024-002. **FINDING** (Weaknesses in Disaster Recovery Planning)

The Legislative Information System (System) had weaknesses over its disaster recovery plan.

The System carries out its mission through the use of Information Technology (IT), including a myriad of applications.

During our testing, we noted the System maintained a disaster recovery plan (Plan); however, the System had not:

- Conducted the Plan testing exercises.
- Performed a Business Impact Analysis (BIA).
- Maintained detailed recovery scripts in the Plan.

The *Contingency Planning Guide for Federal Information Systems* (Special Publication 800-34, First Revision) published by the National Institute of Standards and Technology (NIST), Conduct the Business Impact Analysis and Recovery Phase sections, requires entities to maintain detailed recovery scripts and regularly (at least annually) tested disaster contingency plan to ensure the timely recovery of applications and data. In addition, a detailed 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 to maintain accountability over the State's resources.

System officials stated they were unable to conduct the disaster recovery testing due to budget constraints and did not maintain a BIA due to not being aware of this requirement.

Failure to have an adequately detailed and tested disaster recovery plan and not performing a BIA could result in delayed recovery of the System's operations and affect the System's ability to fulfill its mission. (Finding Code No. 2024-002)

RECOMMENDATION

We recommend the System:

- conduct annual testing of the Plan.
- perform a business impact analysis to identify RPO (Recovery Point Objective), RTO (Recovery Time Objective), and MTD (Maximum Tolerable Downtime) for all of its critical business processes, systems and applications.

2024-002. **FINDING** (Weaknesses in Disaster Recovery Planning) – Continued

- maintain detailed recovery scripts in the Plan for the expedient recovery of systems in the event of a disaster.

SYSTEM RESPONSE

The System accepts the recommendation.

2024-003. **FINDING** (Weaknesses in Change Control Processes)

The Legislative Information System (System) did not have adequate controls over its change management process and had not adequately controlled developers' access to the production environment.

The System had established a change management process describing the change controls from initiation to implementation of changes. However, during the review of the System's change control policies and procedures, we noted the System had not established requirements to conduct post-implementation reviews for emergency changes.

Additionally, during testing we noted the following:

- 3 of 51 (6%) change requests did not follow the System's change control procedures.
- 4 of 4 (100%) developers had privileges to push the code 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, Configuration Management, System and Communications Protection (SC-2), and System and Services Acquisition (SA-1, SA-3, SA-11) sections, requires entities to develop and document controls over changes, adhere to established change control procedures to ensure successful implementation of changes, and restrict the developer access to production environments to reduce the risk of unauthorized changes.

Further, the Fiscal Control and Internal Auditing Act (30 ILCS 10/3001) requires the System to maintain a system, or systems, of internal fiscal and administrative controls to provide assurance funds, property, and other assets and resources are utilized efficiently and effectively.

System officials stated the cause of the identified deficiencies in change control processes stemmed from historical operational practices prioritizing efficiency and flexibility in deployments over stringent role segregation and formalized documentation. Additionally, System officials noted the IT department did not have enough staff to enforce complete separation of development and deployment duties into distinct teams.

Failure to maintain adequate controls over the System's change management process and allowing developers to access the production environment could increases the risk of unauthorized changes and security risks to its environment, applications, and related data. (Finding Code No. 2024-003)

2024-003. **FINDING** (Weaknesses in Change Control Processes) – Continued

RECOMMENDATION

We recommend the System:

- Establish requirements for post-implementation reviews of emergency changes;
- Ensure the established change control procedures are adhered to; and
- Restrict the developer access to the production environment by following the principles of least privilege and segregation of duties.

SYSTEM RESPONSE

The System accepts the recommendation.

2024-004. **FINDING** (Weaknesses in Controls over System Security)

The Legislative Information System (System) had not implemented adequate security controls over its computing environment.

The System carries out its mission through the use of Information Technology (IT), including various applications, which contain confidential or personal information such as names, addresses, and Social Security numbers.

During our examination of the System's security practices, we noted the System had not:

- Maintained patch management policies and procedures for the entire IT environment.
- Conducted annual user access reviews of System applications.
- Formally adopted policies and procedures for access provisioning, property control, and patch management.

Additionally, we noted the System's IT environment was utilizing operating systems no longer supported.

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), System and Services Acquisition (SA-22), System and Information Integrity (SI-1, SI-2), and Access Control (AC-1, AC-2) sections, requires entities to maintain proper internal controls over the security of the environment and access provisioning.

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 to maintain accountability over the State's resources.

System officials stated the cause of the identified deficiencies primarily resulted from historical informal practices, resource constraints, and a lack of structured, consistent oversight mechanisms due to a focus on operational effectiveness, often handling IT tasks informally or reactively. System officials further stated this approach led to gaps in formal documentation and structured procedures, resulting in inadequate controls over system security areas like patch management, user access reviews, and system lifecycle management.

The lack of adequate controls over system security and access management could lead to the System's confidential and personal information being susceptible to cyber-attacks and unauthorized access and disclosure. Without formally adopting

2024-004. **FINDING** (Weaknesses in Controls over System Security) – Continued

the policies, the System may not be able to enforce the existing ad-hoc policies. (Finding Code No. 2024-004)

RECOMMENDATION

We recommend the System:

- Maintain patch management procedures covering the entire IT environment.
- Conduct periodic, at least annual, reviews of user access to System applications.
- Formally adopt all policies and procedures followed by the System.
- Upgrade the operating systems to vendor-supported versions.

SYSTEM RESPONSE

The System accepts the recommendation.

STATE OF ILLINOIS
LEGISLATIVE INFORMATION SYSTEM
SCHEDULE OF FINDINGS – PRIOR FINDINGS NOT REPEATED
For the Two Years Ended June 30, 2024

A. **FINDING** (Inadequate Controls over Personal Services)

During the prior examination, the Legislative Information System (System) did not have adequate controls over personal services.

During the current examination, our sample testing resulted in fewer exceptions which were reported in the System's *Independent Accountant's Report of Immaterial Findings*. (Finding Code No. 2022-001)

B. **FINDING** (Inadequate Internal Controls over Census Data)

During the prior examination, the System did not maintain adequate controls over their census data reconciliations.

During the current examination, our testing indicated the System implemented adequate internal controls related to their census data reconciliations (Finding Code No. 2022-002).

C. **FINDING** (Inadequate Controls over Reconciliations)

During the prior examination, the System did not maintain adequate controls over its monthly reconciliations of the System's contract and expenditure information to the Office of Comptroller's (Comptroller) *Obligation Activity Report* (SC15), expenditure records to the Comptroller's *Monthly Appropriation Status Report* (SB01), and receipt records to the Comptroller's *Monthly Revenue Status* (SB04) report.

During the current examination, our testing indicated the System implemented adequate internal controls related to their reconciliations. In addition, reconciliations of the System's contract and expenditure information to the Comptroller's SC15 were no longer required. (Finding Code No. 2022-003).