

**State of Illinois**  
**Illinois Student Assistance Commission**

**State Compliance Examination**  
**For the Two Years Ended June 30, 2022**

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

**STATE OF ILLINOIS  
ILLINOIS STUDENT ASSISTANCE COMMISSION  
STATE COMPLIANCE EXAMINATION  
For the Two Years Ended June 30, 2022**

**TABLE OF CONTENTS**

<b><i>State Compliance Examination Report</i></b>	<b><u>Page</u></b>
Commission Officials	1
Management Assertion Letter	2
State Compliance Report Summary	3
Independent Accountant's Report on State Compliance and on Internal Control over Compliance	4
Schedule of Findings Current Findings	7
Prior Findings Not Repeated	10

**State of Illinois  
Illinois Student Assistance Commission**

**Commission Officials**

---

Executive Director	Eric Zarnikow
Chief Financial Officer	Shoba Nandhan
Chief Investment Officer	Carmen Heredia-Lopez (07/01/21 – 09/24/22)
Director of Investments	Roger Rojas (09/25/22 – Present)
General Counsel	Karen Salas (07/01/21 – 12/31/21)
Interim General Counsel	Rich Nowell (01/01/22 – Present)
Chief Internal Auditor	Kishor Desai

Commission offices are located at:

1755 Lake Cook Road  
Deerfield, IL 60015

500 West Monroe  
Springfield, IL 62704

100 West Randolph  
Suite N-100  
Chicago, IL 60601



MANAGEMENT ASSERTION LETTER

May 23, 2023

Crowe LLP
One Mid America Plaza
Oak Brook, Illinois 60522-3697

Ladies and Gentlemen:

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, Illinois Student Assistance Commission (Commission). 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 Commission's compliance with the following specified requirements during the two-year period ended June 30, 2022. Based on this evaluation, we assert that during the years ended June 30, 2021, and June 30, 2022, the Commission has materially complied with the specified requirements listed below.

- A. The Commission 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 Commission 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 Commission 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 Commission 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 Commission on behalf of the State or held in trust by the Commission 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, Illinois Student Assistance Commission

SIGNED ORIGINAL ON FILE

Eric Zarnikow, Executive Director

SIGNED ORIGINAL ON FILE

Shoba Nandhan, Chief Financial Officer

SIGNED ORIGINAL ON FILE

Digitally signed by Richard K... 2023.05.23 09:39:52 -05'00'

Rich Nowell, Interim General Counsel

**STATE OF ILLINOIS  
ILLINOIS STUDENT ASSISTANCE COMMISSION  
STATE COMPLIANCE EXAMINATION  
For the Two Years Ended June 30, 2022**

**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**

<b>Number of</b>	<b><u>Current Report</u></b>	<b><u>Prior Report</u></b>
Findings	2	2
Repeated Findings	0	1
Prior Recommendations Implemented or Not Repeated	2	0

**SCHEDULE OF FINDINGS**

<u>Item No.</u>	<u>Page</u>	<u>Last/First Reported</u>	<u>Description</u>	<u>Finding Type</u>
<b>Current Findings</b>				
2022-001	7-8	2022/2022	Weaknesses in Cybersecurity Programs and Practices	Significant Deficiency / Noncompliance
2022-002	9	2022/2022	Lack of Adequate Controls over the Monitoring of Service Providers	Significant Deficiency / Noncompliance
<b>Prior Findings Not Repeated</b>				
A	10	2020/2009	Debt Covenant Violation	
B	10	2020/2020	Lack of Census Data Reconciliations	

**EXIT CONFERENCE**

The Commission waived an exit conference in a correspondence from Shoba Nandhan, Chief Financial Officer, on May 22, 2023. The responses to the recommendations were provided by Dana Mills Danner, Audit Liaison, in a correspondence dated May 22, 2023.

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

Honorable Frank J. Mautino  
Auditor General  
State of Illinois

and

Governing Board  
State of Illinois, *Illinois Student Assistance Commission*

**Report on State Compliance**

As Special Assistant Auditors for the Auditor General, we have examined compliance by the State of Illinois, Illinois Student Assistance Commission (the Commission) 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, 2022. Management of the Commission is responsible for compliance with the specified requirements. Our responsibility is to express an opinion on the Commission's compliance with the specified requirements based on our examination.

The specified requirements are:

- A. The Commission 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 Commission 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 Commission 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 Commission 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 Commission on behalf of the State or held in trust by the Commission 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 Commission complied with the specified requirements in all material respects. An examination involves performing procedures to obtain evidence about whether the Commission complied with the specified requirements. The nature, timing, 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 Commission's compliance with the specified requirements.

In our opinion, the Commission complied with the specified requirements during the two years ended June 30, 2022, 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 2022-001 and 2022-002.

The Commission's responses to the compliance findings identified in our examination are described in the accompanying Schedule of Findings. The Commission'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 Commission 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 Commission's internal control to determine the examination procedures that are appropriate in the circumstances for the purpose of expressing our opinion on the Commission's compliance with the specified requirements and to test and report on the Commission's internal control in accordance with the *Audit Guide*, but not for the purpose of expressing an opinion on the effectiveness of the Commission's internal control. Accordingly, we do not express an opinion on the effectiveness of the Commission'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 2022-001 and 2022-002 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 Commission's responses to the internal control findings identified in our examination are described in the accompanying Schedule of Findings. The Commission'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**

Crowe LLP

Oak Brook, Illinois  
May 23, 2023



**STATE OF ILLINOIS  
ILLINOIS STUDENT ASSISTANCE COMMISSION  
SCHEDULE OF FINDINGS – CURRENT FINDINGS  
For the Two Years Ended June 30, 2022**

**2022-001      FINDING (Weaknesses in Cybersecurity Programs and Practices)**

The Illinois Student Assistance Commission (Commission) had not implemented adequate internal controls related to cybersecurity programs and practices.

The Commission relies on computer systems containing confidential and personal information such as names, addresses, and social security numbers of the citizens of the State for meeting their mission of providing Illinois students with information and assistance to help make education beyond high school accessible and affordable.

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

- Ensured policy reviews were defined.
- Established a data classification methodology, including specific guidelines addressing classification criteria and security methods related to the various classifications.
- Conducted a comprehensive risk assessment.

In addition, our testing noted employees had not completed all monthly cybersecurity awareness training.

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 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.

Commission management indicated they believed the risk assessment process was reasonable and the other weaknesses were due to oversight.

The lack of adequate cybersecurity programs and practices could result in unidentified risk and vulnerabilities, which could ultimately lead to the Commission's confidential and personal information being susceptible to cyber-attacks and unauthorized disclosure. (Finding Code No. 2022-001)

**RECOMMENDATION**

We recommend the Commission:

- Establish a defined frequency for policy reviews;
- Establish a data classification methodology, including specific guidelines addressing classification criteria and security methods related to the various classifications;

**STATE OF ILLINOIS  
ILLINOIS STUDENT ASSISTANCE COMMISSION  
SCHEDULE OF FINDINGS – CURRENT FINDINGS  
For the Two Years Ended June 30, 2022**

**2022-001      FINDING (Weaknesses in Cybersecurity Programs and Practices) (Continued)**

- Conduct a comprehensive risk assessment; and,
- Ensure all employees complete the monthly cybersecurity training.

**COMMISSION RESPONSE**

Management agrees with the findings and will take appropriate actions to remediate the findings.

Establish a frequency for policy reviews – Agency policies are reviewed and updated on a periodic basis and also when the need arises. Agency policy will be updated to add a section for frequency of policy reviews.

Data classification methodology – The Commission’s data classification is specified in the Information System Security Plan. The Information System Security Plan will be updated to include elements with definition and classification.

Comprehensive risk assessment – The Commission works with the Department of Information Technology (DoIT) to conduct a formal risk assessment based on National Institute of Standards and Technology (NIST) . In addition, an informal monthly internal risk assessment is also performed. The most recent risk assessment was conducted in November 2022 which included all systems with a high security rating. The Commission will work with DoIT to conduct a formal comprehensive risk assessment that includes all systems based on DoIT’s availability.

Monthly security awareness training reporting – The Commission has implemented a monthly security awareness training since 2014. This is in addition to the annual security awareness training provided by DoIT. Every month, for staff who doesn’t complete the training on time, automated escalation emails are sent with a copy to their manager on a daily basis till the staff member completes the training. If the staff member leaves the agency, is on vacation, sick or on leave of absence, the training may not be completed by the end of the month. However, when they return, the training is completed. The Commission’s Information Security team has modified the email escalation to notify a week before the end of the training to be proactive. In addition, the Information Security team will work with the security awareness training vendor to address any training completion reporting deficiencies.

**STATE OF ILLINOIS  
ILLINOIS STUDENT ASSISTANCE COMMISSION  
SCHEDULE OF FINDINGS – CURRENT FINDINGS  
For the Two Years Ended June 30, 2022**

**2022-002      FINDING (Lack of Adequate Controls over the Monitoring of Service Providers)**

The Illinois Student Assistance Commission (Commission) had not established adequate controls over the monitoring of service providers.

During the examination period, the Commission utilized six service providers to provide services including student loan servicing, payment processing, collection agency, and hosting services.

During our review, we noted the Commission had not established internal monitoring and oversight procedures to ensure service providers were performing their contracted duties.

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 Service Acquisition sections, requires entities outsourcing their IT environment or operations to employ processes, methods and techniques to monitor compliance of the service providers' contract.

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.

The Commission management indicated they relied on any performance-related issues being timely communicated by Commission employees to management for resolution.

The lack of adequate controls over monitoring of service providers could result in performance weaknesses not being identified and resolved timely. (Finding Code No. 2022-002)

**RECOMMENDATION**

We recommend the Commission establish policies and procedures for monitoring of service providers' performance.

**COMMISSION RESPONSE**

Management agrees with the findings and will take appropriate actions to remediate the findings.

The Contracts and Procurement Policy will be updated to include the Commission's responsibility to monitor contractual responsibilities and deliverables by the service provider.

**STATE OF ILLINOIS  
ILLINOIS STUDENT ASSISTANCE COMMISSION  
SCHEDULE OF FINDINGS – PRIOR FINDINGS NOT REPEATED  
For the Two Years Ended June 30, 2022**

**A. Debt Covenant Violation**

During the prior examination, the Illinois Student Assistance Commission (Commission) – Illinois Designated Account Purchase Program (IDAPP) was not in compliance with the debt ratio covenant relating to the agency's revolving line of credit agreement.

During the current examination, we noted the Commission – IDAPP was in compliance with agreement covenants.(Finding Code No. 2020-001, 2019-001, 2018-001, 2017-001, 2016-001, 2015-001, 2014-001, 2013-001, 12-2, 11-10, 10-6, 09-1)

**B. Lack of Census Data Reconciliations**

In the prior year examination, the Illinois Student Assistance Commission (Commission) did not have a reconciliation process to provide assurance census data submitted to its pension and other postemployment benefits (OPEB) plans was complete and accurate.

In FY21 and reported in the FY21 financial audit report as finding 2021-001, the Commission continued to not have a reconciliation process to provide assurance census data submitted to its pension and other postemployment benefits (OPEB) plans was complete and accurate. After FY21, the Commission has worked with SERS and completed an initial full reconciliation and implemented an annual reconciliation process for census data used in actuarial valuation. No adjustments to Commission records were required based on the reconciliation. (Finding Code No. 2021-001, 2020-002)