

LEGISLATIVE AUDIT COMMISSION



Review of
Governors State University
Year Ended June 30, 2024

620 Stratton Office Building
Springfield, Illinois 62706
(217) 782-7097

REVIEW #4593 GOVERNORS STATE UNIVERSITY – FY24 COMPLIANCE

REVIEW: #4593 GOVERNORS STATE UNIVERSITY YEAR ENDED JUNE 30, 2024

RECOMMENDATIONS – 17

IMPLEMENTED/ PARTIALLY IMPLEMENTED – 17

REPEATED RECOMMENDATIONS – 10

PRIOR AUDIT FINDINGS/RECOMMENDATIONS – 12

This review summarizes the auditors' report of Governors State University of for the year ended June 30, 2024, filed with the Legislative Audit Commission on May 22, 2025. The auditors conducted a compliance examination in accordance with state law and Government Auditing Standards.

Agency Narrative

Governors State University (GSU) was founded in 1969, originally as an upper-division institution with a primary focus of serving community college graduates pursuing baccalaureate degrees. During the five intervening decades, GSU has grown to become the only regional, public, comprehensive university in Chicago's south suburban area

GSU is led by Dr. Joyce Ester, who began on July 1, 2025. Before her appointment as President of Governors State University, Dr. Ester served as President of Normandale Community College in Minnesota—the state's largest community college. Prior to Normandale, Dr. Ester served as President of Kennedy-King College, one of the seven City Colleges of Chicago, where she led initiatives focused on student success, workforce development, and community engagement. A native of Phoenix, Illinois, Dr. Ester holds a bachelor's degree in Sociology from Northern Illinois University and both a master's and a doctorate in Education from the University of California, Santa Barbara.

Dr. Cheryl Green served as President from July 2020 until she retired on March 1, 2025. Dr. Green passed away on April 23, 2025, after a long battle with cancer.

Appropriations and Expenditures

Appropriations (\$ thousands)	FY23		FY24	
	Approp	Expend	Approp	Expend
GENERAL FUNDS				
Operational Expenses	24,353.3	24,353.3	26,058.1	26,058.1
TOTAL GENERAL FUNDS	24,353.3	24,353.3	26,058.1	26,058.1

REVIEW #4593 GOVERNORS STATE UNIVERSITY – FY24 COMPLIANCE

Accountants' Findings and Recommendations

Condensed below are the 17 findings and recommendations included in the audit report. Of these, ten are repeated from the previous audit. The following recommendations are classified on the basis of information provided by Governors State University, via electronic mail received May 22, 2025.

- 1. The auditors recommend the University update its policies and procedures to describe testing and documentation requirements for each type of change.**

Further, they recommend the University strengthen controls to ensure proper segregation of duties are established by restricting developers' access to the production environment.

FINDING: *(Weaknesses in Change Control Processes) – First reported 2023, Last reported 2024*

Governors State University (University) did not have adequate controls around its change control process and had not adequately controlled developer access to its production environment.

The University established a change management process describing the process from initiation until post-implementation review. However, during the review of the University's change control policies and procedures, the auditors noted the following:

- The change policy did not describe standard testing and documentation requirements for each type of change.
- Developers had access to the production environment, resulting in a segregation of duties weakness.

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 and System and Communication Protection sections, requires entities to develop and document control over changes, for changes to follow the documented controls, and developers' access to the production environment is restricted.

Further, the Fiscal Control and Internal Auditing Act (30 ILCS 10/3001) requires the University to maintain a system, or systems, of internal fiscal and administrative controls with proper segregation of duties to provide assurance that resources are utilized efficiently and effectively.

University officials stated these exceptions were due to resource constraints and competing priorities.

REVIEW #4593 GOVERNORS STATE UNIVERSITY – FY24 COMPLIANCE

Failure to establish adequate controls and documentation around the change control process may lead to the University being unable to monitor and ensure only valid, authorized changes are deployed in the University's Information Technology Environment. Also, allowing developers to access the production environment results in segregation of duties weakness and increases the risk of unauthorized changes being made to the computing system.

UNIVERSITY RESPONSE:

The University agrees with this finding and accepts the recommendation. The University has built a robust change control program to ensure system changes are completed with minimal impact and security implications. The University will also prioritize establishing the necessary procedures. Additionally, the University plans to engage with a third party which will be responsible for implementing changes to the Colleague production environment, remedying the separation of duties weakness.

UPDATED RESPONSE:

Implemented.

University procedure has been adopted and includes testing and documentation requirements for each type of change. ITS employees are reminded of the change control procedures in a weekly email. In addition to University procedure adopted, a managed services vendor (Toad Code) has been engaged to apply all Ellucian Colleague updates to the production environment. This ensures segregation of duties by preventing members of the University's Applications Team from applying their own changes to the production environment. All changes must be approved via established change control processes

- 2. The auditors recommend the University improve its procedures to ensure timely and accurate reporting of student enrollment status to the NSLDS both in Program-Level Record and Campus-Level Record.**

FINDING: *(Enrollment Reporting) – This finding has been repeated since 2021.*

Federal Department:	U.S. Department of Education
Assistance Listing Number:	84.268
Cluster Name:	Student Financial Assistance Cluster
Program Name:	Federal Direct Student Loans
Award Numbers:	P268K240567, P268K230567
Questioned Cost:	None
Program Expenditures:	\$21,113,430
Cluster Expenditures:	\$32,781,904

Governors State University (University) did not timely and accurately report student enrollment information to the U.S. Department of Education's National Student Loan Data System (NSLDS).

REVIEW #4593 GOVERNORS STATE UNIVERSITY – FY24 COMPLIANCE

During testing of 40 enrollment status changes, the auditors noted the following:

- Seven of 40 (18%) enrollment status changes were not reported timely to the NSLDS. These enrollment status changes were reported 1 to 228 days late after the date of occurrence. In addition, 2 of the 7 enrollment status changes pertain to students with direct loans who ceased to be enrolled on at least a half-time basis for the period for which the loan was intended.
- Ten of 40 (25%) enrollment status changes data had discrepancies in Program Begin Date ranging from 1,254 days early to 2 days late when compared to their official program start dates.

The sample was not intended to be, and was not, a statistically valid sample.

The Code of Federal Regulations (34 CFR 685.309) requires the University, upon the receipt of an enrollment report from the Secretary of the Department of Education (ED), to update all information included in the report and return the report to the ED within the timeframe prescribed by the ED. It further requires the University to report enrollment changes within 30 days unless a roster file is expected within 60 days, in which case the enrollment data may be updated on that roster file changes. This report should include changes such as when a Direct Loan was made to or on behalf of a student who was enrolled or accepted for enrollment at the University, and the student has ceased to be enrolled on at least a half-time basis or failed to enroll on at least a half-time basis for the period for which the loan was intended.

The NSLDS Enrollment Reporting Guide states the University is responsible for accurately reporting all Program-Level Record and Campus-Level Record data elements. The Program Begin Date is the date the student first began attending the program being reported. Typically, this would be the first day of the term in which the student began enrollment in the program, unless the student enrolled in the program on an earlier date.

The Uniform Guidance (2 CFR 200.303) requires nonfederal entities receiving federal awards to establish and maintain internal controls designed to reasonably ensure compliance with federal statutes, regulations, and terms and conditions of the federal award. Effective internal controls should include procedures to ensure accurate and timely student enrollment status reports are submitted to NSLDS.

University officials stated the delay in reporting status changes was attributable to challenges within the reporting protocols to the NSLDS for various status change scenarios occurring after the term end date and delays in the internal reporting process.

The University reports enrollment status changes to NSLDS through the National Student Clearinghouse (NSC), a third-party servicer. As part of the enrollment reporting process, system-generated files are uploaded to the NSC, which then provides the data to NSLDS. Upon review of the system-generated files, there are various dates contained within the files, which may have caused inaccurate Program Begin Dates reflected in the NSLDS' Program-Level Record.

REVIEW #4593 GOVERNORS STATE UNIVERSITY – FY24 COMPLIANCE

Accurate, timely, and complete enrollment information is critical for effective and proper administration of the student financial aid programs. Noncompliance with enrollment reporting regulations may result in a loss of future federal funding.

UNIVERSITY RESPONSE:

The University agrees with this finding and accepts the recommendation. Following consultation with the NSC, guidelines were provided for handling various status change scenarios. These guidelines will enhance the accuracy of enrollment status change reporting, particularly for students with changes occurring before or after the subsequent enrollment file submission. Status changes are now being reported to the NSLDS in a timely and accurate manner, in accordance with the NSC guidelines. The University has also implemented a reporting timeline and review protocols to ensure status changes are reported to the NSLDS in a timely manner. Additionally, the University will collaborate with its Information Technology Services and representatives from the NSC and NSLDS to verify the accuracy of the file layouts and the data flow of the information provided.

UPDATED RESPONSE:

Implemented.

3. The auditors recommend the University continue towards completion and full implementation of the written incident response plan.

FINDING: *(Noncompliance with Gramm-Leach-Bliley Act) – First reported 2023, Last reported 2024*

Federal Department:	U.S. Department of Education, U.S. Department of Health and Human Services
Assistance Listing Number:	84.268, 84.063, 84.038, 84.033, 84.007, 84.379, 93.925, 93.264
Cluster Name:	Student Financial Assistance Cluster
Program Name:	Federal Direct Student Loans, Federal Pell Grant Program, Federal Perkins Loan Program, Federal Work-Study Program, Federal Supplemental Educational Opportunity Grants, Teacher Education Assistance for College and Higher Education Grants, Scholarships for Health Professions Students from Disadvantaged Backgrounds, and Nurse Faculty Loan Program
Award Numbers:	P268K240567, P268K230567, P063P230567, P063P220567, P033A231156, P033A221156, P007A231156, P007A221156, P379T240567, 5 T08HP39308-04-00, and E01HP27019
Questioned Cost:	None
Program Expenditures:	\$21,113,430; \$7,760,752; \$1,938,618; \$512,881; \$227,850; \$31,236; \$576,000; \$621,137

REVIEW #4593 GOVERNORS STATE UNIVERSITY – FY24 COMPLIANCE

Cluster Expenditures: \$32,781,904

Governors State University (University) did not establish a written incident response plan designed to promptly respond to, and recover from, any security event materially affecting the confidentiality, integrity, or availability of customer information in their control.

During their audit, the auditors noted the University was unable to complete the development of the written incident response plan as of the end of the audit period.

On December 9, 2021, the Federal Trade Commission issued final regulations to amend the Standards for Safeguarding Customer Information (Safeguards Rule), an important component of the Gramm-Leach-Bliley Act's (GLBA) requirements for protecting the privacy and personal information of consumers.

The Code of Federal Regulations (16 CFR 314.4(h)) requires the University to develop, implement and maintain an information security program which includes establishing a written incident response plan designed to promptly respond to, and recover from, any security event materially affecting the confidentiality, integrity, or availability of customer information in its control.

At a minimum, such incident response plan shall address the following areas:

- the goals of the incident response plan;
- the internal processes for responding to a security event;
- the definition of clear roles, responsibilities, and levels of decision-making authority;
- external and internal communications and information sharing;
- identification of requirements for the remediation of any identified weaknesses in information systems and associated controls;
- documentation and reporting regarding security events and related incident response activities; and
- the evaluation and revision as necessary of the incident response plan following a security event.

Additionally, the Uniform Guidance (2 CFR 200.303(a)) requires nonfederal entities receiving federal awards to establish and maintain effective internal control designed to reasonably ensure compliance with federal laws, statutes, regulations, and the terms and conditions of the federal award.

University officials stated the University has been actively engaged in the development of a written incident response plan; however, the plan was not completed by the end of Fiscal Year 2024 due to the extensive range of tasks required for its completion.

The intent of the GLBA Safeguards Rule is to enhance security over confidential information. Without a documented response to all applicable requirements, the

REVIEW #4593 GOVERNORS STATE UNIVERSITY – FY24 COMPLIANCE

University is more susceptible to vulnerabilities as it relates to protecting the privacy and personal information of students than it will be following full implementation.

UNIVERSITY RESPONSE:

The University agrees with this finding and accepts the recommendation. The University has recently completed the development of the written incident response plan during Fiscal Year 2025.

UPDATED RESPONSE:

Implemented.

The Incident Response Plan has been completed and adopted.

- 4. The auditors recommend the University improve its procedures to ensure proper notification is made to the parent Direct PLUS borrowers.**

FINDING: *(Noncompliance with Notification Requirements on Direct PLUS Loans Disbursements) - New*

Federal Department:	U.S. Department of Education
Assistance Listing Number:	84.268
Cluster Name:	Student Financial Assistance Cluster
Program Name:	Federal Direct Student Loans
Award Numbers:	P268K240567, P268K230567
Questioned Cost:	None
Program Expenditures:	\$21,113,430
Cluster Expenditures:	\$32,781,904

Governors State University (University) did not comply with the notification requirements on Direct PLUS Loans disbursements.

During testing of 25 Direct Loans disbursements, the auditors noted 2 (8%) students with Direct PLUS loans, where the parents were not properly notified. Notifications were made only to students.

The Code of Federal Regulations (34 CFR 668.165) requires the University when Direct Loans are being credited to a student's account to notify the student, or parent, in writing of (1) the date and amount of the disbursement; (2) the student's right, or parent's right, to cancel all or a portion of that loan or loan disbursement and have the loan proceeds returned to Department of Education; and (3) the procedure and time by which the student or parent must notify the institution that he or she wishes to cancel the loan (a minimum of 14 or 30 days depending on confirmation process). Further, the Federal Student Aid (FSA) handbook clarified that general notification must be provided to the parent Direct PLUS borrower and all students receiving FSA funds.

University officials stated they were aware of the notification requirements and believed the existing process was compliant with the requirements.

REVIEW #4593 GOVERNORS STATE UNIVERSITY – FY24 COMPLIANCE

Proper notifications protect the borrower's rights and give the parent borrower a chance to reconsider the loan, adjust disbursements or cancel within the specified timeframe. In addition, failure to implement notification requirements represents noncompliance with federal regulations.

UNIVERSITY RESPONSE:

The University agrees with this finding and accepts the recommendation. The University has implemented changes to procedures to send proper notification to the parent Direct PLUS borrowers.

UPDATED RESPONSE:

Implemented.

5. The auditors recommend the University improve its procedures to ensure documentation is retained to demonstrate timely completion of reconciliations.

FINDING: *(Failure to Retain Adequate Documentation of Internal Direct Loans Reconciliation) - New*

Federal Department:	U.S. Department of Education
Assistance Listing Number:	84.268
Cluster Name:	Student Financial Assistance Cluster
Program Name:	Federal Direct Student Loans
Award Numbers:	P268K240567, P268K230567
Questioned Cost:	None
Program Expenditures:	\$21,113,430
Cluster Expenditures:	\$32,781,904

Governors State University (University) did not retain documentation of its internal monthly Direct Loans reconciliation to demonstrate timely completion.

During testing of Direct Loans, the auditors were unable to verify whether the University completed the monthly internal reconciliation in a timely manner due to the absence of supporting documentation.

The Federal Student Aid (FSA) issued Electronic Announcement General-22-86 covering reconciliation requirements for all Title IV programs between Department of Education's G5 system records and the University's internal records. It further requires the University to reconcile internally, disbursement data between Financial Services and Comptroller Office and Financial Aid Office.

Additionally, the Uniform Guidance (2 CFR 200.303(a)) requires nonfederal entities receiving federal awards to establish and maintain effective internal control designed to

REVIEW #4593 GOVERNORS STATE UNIVERSITY – FY24 COMPLIANCE

reasonably ensure compliance with federal laws, statutes, regulations, and the terms and conditions of the federal award.

University officials stated the University performs the monthly internal reconciliation process. However, the monthly internal reconciliation spreadsheet is updated each month without retaining the prior versions.

Failure to properly document internal monthly reconciliations between the Financial Services and Comptroller Office and Financial Aid Office may result in inaccurate and incomplete financial information.

UNIVERSITY RESPONSE:

The University agrees with this finding and accepts the recommendation. Existing procedures have been revised to require the retention of internal reconciliation records on a monthly basis.

UPDATED RESPONSE:

Implemented.

- 6. The auditors recommend the University improve its procedures to ensure compliance with records retention requirements.**

FINDING: *(Noncompliance with Perkins Loans' Retention of Records Requirements) – New*

Federal Department:	U.S. Department of Education
Assistance Listing Number:	84.038
Cluster Name:	Student Financial Assistance Cluster
Program Name:	Federal Perkins Loan Program
Award Number:	None
Questioned Cost:	None
Program Expenditures:	\$1,938,618
Cluster Expenditures:	\$32,781,904

Governors State University (University) did not maintain a copy of the master promissory note (MPN) for a Perkins Loan program loan.

During testing of Perkins Loan receivables, the auditors identified 1 of 12 (8%) students with a missing MPN.

The Code of Federal Regulations (34 CFR 674.19(e)) requires the University to retain a record of disbursements for each loan made to a borrower on a promissory note. In addition, the University is required to keep the original MPN until the loans are satisfied. If required to release original documents in order to enforce the loan, the University must retain certified true copies of those documents.

REVIEW #4593 GOVERNORS STATE UNIVERSITY – FY24 COMPLIANCE

University officials stated the University maintains copies of the MPNs; however, the one MPN pertained to a Perkins Loan disbursed over 18 years ago. Consequently, it may have been misplaced due to staffing changes over the years.

Failure to properly maintain loan documentation may result in inaccurate loan balances, potential disputes with borrowers, and noncompliance with federal regulations.

UNIVERSITY RESPONSE:

The University agrees with this finding and accepts the recommendation. Existing University procedures ensure MPNs and other Perkins-related documentation requirements are properly maintained. The University will continue its ongoing process of reviewing Perkins's documentation to comply with the requirements.

UPDATED RESPONSE:

Implemented.

- 7. The auditors recommend the University improve its procedures to ensure fringe benefits allocated to the grant align consistently with the salaries and wages charged to the grant.**

FINDING: *(Noncompliance with Activities Allowed or Unallowed and Allowable Costs and Cost Principles Requirements) - New*

Federal Department:	U.S. Department of Education
Assistance Listing Number:	84.425D
Cluster Name:	Education Stabilization Fund
Program Name:	Elementary and Secondary School Emergency Relief Fund
Award Number:	S425D210041
Questioned Cost:	None
Program Expenditures:	\$1,222,010
Cluster Expenditures:	\$1,466,030

Governors State University (University) did not comply with activities allowed or unallowed and allowable costs and cost principles requirements.

During their review of the Illinois Tutoring Initiative program under the Elementary and Secondary School Emergency Relief (ESSER) Fund which had total expenditures of \$1,222,010, the auditors identified 1 of 25 (4%) expenditures was inappropriately charged to the grant. The University inadvertently charged Central Management Services (CMS) insurance of \$414 for an employee who did not work on the program. The sample was not intended to be, and was not, a statistically valid sample.

The Code of Federal Regulations (2 CFR 200.431(c)) requires the University to allocate fringe benefits to federal awards and all other activities in a manner consistent with the pattern of benefits attributable to the individuals or group(s) of employees whose salaries

REVIEW #4593 GOVERNORS STATE UNIVERSITY – FY24 COMPLIANCE

and wages are chargeable to such federal awards and other activities, and charged as direct or indirect costs following the University's accounting practices.

Additionally, the Uniform Guidance (2 CFR 200.303(a)) requires nonfederal entities receiving federal awards to establish and maintain effective internal control designed to reasonably ensure compliance with federal laws, statutes, regulations, and the terms and conditions of the federal award.

University officials stated the charge was meant for a different federal grant, but was inadvertently assigned to the ESSER grant due to a formula error in the supporting spreadsheet.

Failure to accurately charge the correct grant may result in disallowance of federal expenditures and questioned costs, and could jeopardize future federal funding.

UNIVERSITY RESPONSE:

The University agrees with this finding and accepts the recommendation. More stringent review procedures have been implemented to prevent the recurrence of this issue.

UPDATED RESPONSE:

Implemented.

- 8. The auditors recommend the University continue to focus on the incremental changes to the census data file from the prior actuarial valuation, provided no risks are identified that incomplete or inaccurate reporting of census data may have occurred during prior periods. Any errors identified during this process should be promptly corrected by either the University or SURS, with the impact of these errors communicated to both SURS' actuary and CMS' actuary.**

Further, they recommend the University ensure all events occurring within a census data accumulation year are timely reported to SURS so these events can be incorporated into the census data provided to SURS' actuary and CMS' actuary.

FINDING: *(Inadequate Internal Controls over Census Data) – This finding has been repeated since 2020.*

The Governors State University (University) did not have adequate internal control over reporting its census data to provide assurance census data submitted to its pension and other postemployment benefits (OPEB) plans was complete and accurate.

Census data is demographic data (date of birth, gender, years of service, etc.) of the active, inactive, or retired members of a pension or OPEB plan. The accumulation of inactive or retired members' census data occurs before the current accumulation period of census data used in the plan's actuarial valuation (which eventually flows into each employer's financial statements), meaning the plan is solely responsible for establishing

REVIEW #4593 GOVERNORS STATE UNIVERSITY – FY24 COMPLIANCE

internal controls over these records and transmitting the data to the plan's actuary. In contrast, responsibility for active members' census data during the current accumulation period is split among the plan and each member's current employer(s). Initially, employers must accurately transmit census data elements of their employees to the plan. Then, the plan must record and retain these records for active employees and then transmit this census data to the plan's actuary.

The auditors noted the University's employees are members of the State Universities Retirement System (SURS) for their pensions and the State Employees Group Insurance Program sponsored by the State of Illinois, Department of Central Management Services (CMS) for their OPEB. In addition, they noted these plans have characteristics of different types of pensions and OPEB plans, including single employer plans and cost-sharing multiple-employer plans. Additionally, CMS' actuary uses census data for employees of the State's public universities provided by SURS, along with census data for the other participating members provided by the State's four other pensions plans, to prepare their projection of the liabilities of CMS' plan. Finally, SURS' actuary and CMS' actuary used census data transmitted by the University during Fiscal Year 2022 to project pension and OPEB-related balances and activity at the plans during Fiscal Year 2023, which is incorporated into the University's Fiscal Year 2024 financial statements.

During their cut-off testing of data transmitted by the University to SURS, the auditors noted 3 instances of an inactive employee becoming active were reported to SURS after the close of the fiscal year in which the event occurred. These instances have been previously reported, however still impacted the June 30, 2022 census data. SURS determined the total potential impact of these errors was the instructors' service credit was off by a combined 6.75 years.

The auditors provided SURS' actuary and CMS' actuary with the exceptions they identified during their testing, along with the results of census data testing at the State Employees Retirement System of Illinois, and determined the net effect of these errors, along with the errors of other plan participants, was immaterial to SURS' and CMS' pension and OPEB-related balances and activity at the plans during Fiscal Year 2023.

The Fiscal Control and Internal Auditing Act (30 ILCS 10/3001) requires the University to establish and maintain a system, or systems, of internal fiscal and administrative controls to provide assurance funds applicable to operations are properly recorded and accounted for to permit the preparation of reliable financial reports and to maintain accountability over the State's resources.

University officials indicated the 3 instances of late reported events occurred before the current procedures were put into place.

Failure to ensure complete and accurate census data was reported to SURS reduces the overall reliability of pension and OPEB-related balances and activity reported in the University's financial statements, the financial statements of other employers within both plans, and the State of Illinois' Annual Comprehensive Financial Report.

REVIEW #4593 GOVERNORS STATE UNIVERSITY – FY24 COMPLIANCE

UNIVERSITY RESPONSE:

The University agrees with this finding and accepts the recommendation. The University has already established procedures that will address timely and accurate reporting of census data events to SURS.

UPDATED RESPONSE:

Implemented.

The University developed SURS eligibility procedures and trained appropriate Human Resources staff about census data submittal to SURS.

- 9. The auditors recommend the University strengthen its internal controls to ensure partial tuition waivers for children of University employees comply with statutory limits. In addition, they recommend the University seek repayment of waived tuition amount.**

FINDING: *(Inadequate Controls over Monitoring of Partial Tuition Waivers) – New*

The Governors State University (University) did not maintain adequate controls over monitoring of partial tuition waivers granted to children of University employees.

During their testing of University employee waivers, the auditors noted one of 3 (33%) students selected for testing received partial tuition waiver benefits for more than four years while enrolled at the University and another participating State university. The student exceeded the limit by one academic year or equivalent to \$7,199.

The Governors State University Law (Law) (110 ILCS 670/15-90(c)) states the eligible applicant who has continued to maintain satisfactory academic progress toward graduation may have his or her partial tuition waiver renewed until the time as he or she has expended 4 years of undergraduate partial tuition waiver benefits.

University officials stated the University lacked formal procedures for administering dependent tuition waivers.

Failure to monitor tuition waivers resulted in financial loss to the University and noncompliance with the Law.

UNIVERSITY RESPONSE:

The University agrees with this finding and accepts the recommendation. The University has begun updating its process to comply with the mandate by requiring students complete the new form and implementing regular monitoring procedures of each waiver submitted. Written procedures will also be developed to ensure staff members processing dependent tuition waivers understand the process.

UPDATED RESPONSE:

Partially Implemented.

REVIEW #4593 GOVERNORS STATE UNIVERSITY – FY24 COMPLIANCE

New forms have been developed and are currently in use. An additional review of all submitted waivers will be conducted just before the start of each semester. University procedures are currently being developed with completion expected by December 2025.

- 10. The auditors recommend the University maintain the report on file along with all supporting documentation to ensure accurate record keeping and compliance with the Act.**

FINDING: *(Inadequate Internal Controls over Compliance with College Student Immunization Act) – New*

The Governors State University (University) did not have adequate internal control over compliance with the College Student Immunization Act (Act).

During the auditors review of the University's annual immunization report for Fall 2023 covered students, the University did not retain the supporting population immunization records of enrolled students.

As a result, they were unable to perform detailed testing of the University's immunization records as reported to the Illinois Department of Public Health (Department), and unable to determine accuracy of the annual immunization report submitted by the University.

The Act (110 ILCS 20/5) requires the University to maintain on file the proof of immunization, certification of medical exemption or statement of religious objection for all persons attending the institution.

The State Records Act (5 ILCS 160/8) requires the University to make and preserve records containing adequate and proper documentation of the functions, policies, decisions, procedures and essential transitions designed to protect the legal and financial rights of the State.

University officials stated their files were inadvertently overwritten when reports were updated. The University's ERP System maintains student immunization data in real time, and it was not possible to run a historical report from a date in the past.

Failure to retain supporting population records of reports submitted to the Department may compromise the University's ability to ensure compliance with the Act and could adversely impact future decision making when such information is required to address public health risks from communicable diseases.

UNIVERSITY RESPONSE:

The University agrees with this finding and accepts the recommendation. Since Fall of 2024, any data source used for Department reporting has been saved in multiple locations with detailed indexes to demonstrate how data was calculated for each reporting section of the College Student Immunization Status Certification Form. This will reduce the possibility of losing or corrupting information that cannot be recreated for prior years.

REVIEW #4593 GOVERNORS STATE UNIVERSITY – FY24 COMPLIANCE

UPDATED RESPONSE: **Implemented.**

11. The auditors recommend the University improve its procedures to ensure timely finalization of its audit documentation. They further recommend the University to conduct a periodic external assessment of the internal audit function, in compliance with the IPPIA standards.

FINDING: *(Internal Audit Deficiencies) – New*

The Governors State University (University) had deficiencies within its internal audit activities during Fiscal Year 2024.

During their testing, the auditors noted the following:

- Three of 4 (75%) audit reports had not been provided to the auditors. Additionally, the internal audit workpapers for two sample audit reports remain outstanding. The University's Chief Internal Auditor (CIA) reported four completed audits in the annual report dated September 30, 2024 to the University President.
- The University's internal audit function failed to conduct a new external assessment during the examination period as required. The last external assessment was conducted in July 2018. Additionally, the annual audit report dated September 30, 2024, incorrectly stated that internal audit engagements were conducted in accordance with International Standards for the Professional Practice of Internal Auditing (IPPIA).

The Fiscal Control and Internal Auditing Act (Act) (30 ILCS 10/2003(a)(1)) requires the CIA to submit a written report to the chief executive officer detailing how the audit plan for that year was carried out, the significant findings, and the extent to which recommended changes were implemented. In addition, the IPPIA Section 2330 requires internal auditors to document sufficient, reliable, relevant, and useful information to support the engagement results and conclusions.

The University's Internal Audit Charter also includes the following in its description of the audit process:

- Adequate documentation supporting the audit procedures performed, the results of testing, analysis, and conclusions.
- A written report of the Office of Internal Audit's evaluation of the risks and controls, including the results of testing, exceptions noted, weaknesses identified, and recommendations.

REVIEW #4593 GOVERNORS STATE UNIVERSITY – FY24 COMPLIANCE

The IPPIA Section 1312 requires external assessments to be conducted at least every five years by a qualified, independent assessor or assessment team from outside the organization.

The IPPIA Section 1321 states “Indicating that the internal audit activity conforms with the International Standards for the Professional Practice of Internal Auditing is appropriate only if supported by the results of the quality assurance and improvement program.”

University officials stated the issues were primarily due to the historical resource constraints within the internal audit function, which operated as a one-person department until June 1, 2023, delays in obtaining the requested information and documents from the auditees, along with competing priorities and ongoing audit engagements. Despite efforts to manage the audit workload, these limitations affected their ability to meet key audit requirements during the audit period. Further, the nonconformance with the IPPIA was communicated to management and Board of Trustees as part of the annual internal audit reporting at the Board of Trustees on March 10, 2025.

Reporting audits as completed when the supporting documentation had not been finalized precludes management from having a clear picture of internal audit activity. In addition, the lack of a periodic external assessment may delay the detection of deficiencies in the internal audit program and results in noncompliance with the IPPIA standards.

UNIVERSITY RESPONSE:

The University agrees with this finding and accepts the recommendation. The Office of Internal Audit is committed to ensuring the efficient completion of planned audits including the preparation of comprehensive supporting documentation, and timely issuance of the reports thereon. As part of the external quality assessment process, the Office of Internal Audit has already initiated the self-assessment phase, which will be followed by independent validation conducted by a qualified, independent external assessor. Furthermore, the Office of Internal Audit has hired an additional staff member to alleviate resource limitations.

UPDATED RESPONSE:

Partially Implemented.

The planned audits have been completed, and the supporting documentation and reports have been finalized. The Office of Internal Audit is currently in the process of completing the external quality assurance review. The self-assessment component of the external quality assessment has been initiated, and the office continues to coordinate the next steps for independent validation.

- 12. The auditors recommend the University revise its procedures, policies, and/or contracts to ensure all employees submit time sheets documenting the time spent each day on official State business to the nearest quarter hour.**

FINDING: *(Time Sheets not Properly Maintained) – This finding has been repeated since 2005.*

REVIEW #4593 GOVERNORS STATE UNIVERSITY – FY24 COMPLIANCE

The Governors State University (University) did not maintain time sheets for its faculty members and advisors in compliance with the State Officials and Employees Ethics Act (Act).

During their testing of 25 employee time sheets. The auditors noted 4 (16%) faculty members/advisors used "negative" timekeeping whereby the employee is assumed to be working unless noted otherwise.

The University was first cited for this noncompliance in the compliance examination for the year ended June 30, 2005. In the years since the finding was first noted, the University has failed to take substantive corrective actions to resolve the condition noted in this finding.

The Act required the Illinois Board of Higher Education (IBHE), with respect to State employees of public universities, to adopt and implement personnel policies. The Act (5 ILCS 430/5-5(c)) states, "The policies shall require State employees to periodically submit timesheets documenting the time spent each day on official State business to the nearest quarter hour; contractual State employees may satisfy the time sheets requirement by complying with the terms of their contract, which shall provide for means of compliance with this requirement." The IBHE adopted personnel policies for public universities on February 3, 2004 in accordance with the Act. The University has not incorporated these policies into the University's policies.

University officials indicated they have not changed timesheet procedures for faculty members and advisors to comply with the Act since its inception, and have continued to review, along with other State universities, time reporting for faculty members and advisors, as it relates to existing collectively bargained contractual obligations. The University's efforts to establish new time reporting requirements for faculty members and advisors in accordance with the Act were completed, but these changes were not implemented until after Fiscal Year 2024.

By not requiring positive time reporting from all its employees, the University is not in compliance with the Act.

UNIVERSITY RESPONSE:

The University agrees with this finding and accepts the recommendation. The University implemented new time reporting requirements effective for the pay period beginning October 1, 2024, mandating that faculty members and advisors submit semi-monthly timesheets documenting the time spent each day on official State business to the nearest quarter hour, in compliance with the Act.

UPDATED RESPONSE:

Implemented.

- 13. The University has the ultimate responsibility for ensuring its information system resources are available for authorized use and confidential**

REVIEW #4593 GOVERNORS STATE UNIVERSITY – FY24 COMPLIANCE

information is protected from accidental or unauthorized disclosure. Specifically, the auditors recommend the University:

- Implement appropriate controls to reduce the risk of unauthorized disclosure in response to risk assessments and vulnerability monitoring.
- Develop the University's security program (formal and comprehensive policies, procedures and processes) to manage and monitor the regulatory, legal, environmental and operational requirements.
- Develop detailed guidance on controls for storage media, access permissions, data retention, and data destruction policies in alignment with the University's classification of data.
- Regularly communicate security policies to employees, students and contractors and maintain a record of such.
- Develop a project management framework to guide the process of developing and implementing new applications.
- Develop written procedures for security event monitoring and maintain a log of security events.

FINDING: *(Weaknesses in Cybersecurity Programs and Practices) – This finding has been repeated since 2019.*

Governors State University (University) had not fully implemented adequate internal controls related to cybersecurity programs and practices.

As a result of the University's mission to provide higher educational opportunities to its student body, the University maintains computer systems that contain large volumes of confidential or personal information such as names, addresses, educational records, and Social Security numbers within its computerized systems.

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

- Documented and implemented appropriate controls to reduce the risk of unauthorized disclosure in response to risk assessments and vulnerability monitoring.
- Developed a formal, comprehensive, and adequate security program (policies, procedures, and processes) to manage and monitor the regulatory, legal, environmental and operational requirements.
- Developed detailed guidance on controls for storage media, access permissions, data retention, and data destruction policies in alignment with the University's classification of data.

REVIEW #4593 GOVERNORS STATE UNIVERSITY – FY24 COMPLIANCE

- Developed formal policies and procedures for dissemination of all of its information system policies to employees, students, and contractors utilizing the University's resources.
- Developed a project management framework to ensure new applications were developed and implemented in accordance with management's intentions.
- Developed and adopted policies and procedures for monitoring and logging of security events.

Finally, this finding was first noted during the University's Fiscal Year 2019 State compliance examination. As such, University management has been unsuccessful in implementing a corrective action plan to remedy this deficiency.

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 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.

Finally, the University's management team is responsible for implementing timely corrective action on all of the findings identified during a State compliance examination.

University officials indicated resource constraints and competing priorities have prevented the development and adoption of formal cybersecurity plan and programs.

The lack of adequate cybersecurity programs and practices could result in unidentified risks and vulnerabilities and ultimately lead to the University's information system resources and volumes of personal information being susceptible to cyber-attacks and unauthorized disclosure.

UNIVERSITY RESPONSE:

The University agrees with this finding and accepts the recommendation, and has taken the following corrective actions:

- The University currently performs an annual risk assessment and continuous vulnerability monitoring of internet-facing systems. Vulnerability monitoring of internal systems has been included in a Request for Proposal (RFP) for a managed security services provider, which is currently in the evaluation phase.
- The University has adopted Policy 92, Information Security, and is adopting additional security-related policies and procedures as appropriate. The University will continue to prioritize the creation of the recommended policies and procedures.

REVIEW #4593 GOVERNORS STATE UNIVERSITY – FY24 COMPLIANCE

- The University now notifies employees and students of new security-related policies and procedures via the quarterly Information Technology Services newsletter. For contractors, an onboarding document has been developed, which includes a link to the University's public policies. This document is planned for distribution to contractors soon.
- A Project Oversight Committee has been formed, and a project management framework is being developed as resource capacity allows.
- Policies and procedures for monitoring and logging of security events are planned pending the outcome of the aforementioned RFP for a managed security services provider.

UPDATED RESPONSE:

Partially Implemented.

Several procedures were adopted during FY25 to strengthen the University's information security program, with additional procedures to be adopted to address the remaining recommendations. A project oversight committee has been formed, along with a dedicated Microsoft Teams site containing project templates and tracking tools. The adoption of formal documentation is expected to begin within the current fiscal year.

Information security policies are publicly accessible, and updates or substantive changes are communicated to all employees and students through the ITS newsletter.

The University is preparing to release the third iteration of the RFP for managed security services. Completion of the RFP process will precede the development of formal procedures for security event monitoring. Known security events are now logged in the ITS ticketing system.

14. The auditors recommend the University establish and adopt formal policies and procedures for physical access security, and monitoring, testing, and installing vendor released patches.

FINDING: *(Computer Security Weaknesses) – This finding has been repeated since 2016.*

Governors State University (University) had not established adequate controls for its computing environment.

During review of the University's controls around system security, the auditors noted the University had not established formal policies and procedures for:

- Restricting physical access to computer resources.
- Monitoring, testing, and installing vendor released patches.

This finding was first noted during the University's Fiscal Year 2016 State compliance examination. As such, University management had been unsuccessful in implementing a corrective action plan to remedy this deficiency.

The *Security and Privacy Controls for Information Systems and Organizations* (Special Publication 800-53, Fifth Revision) published by the National Institute of Standards and

REVIEW #4593 GOVERNORS STATE UNIVERSITY – FY24 COMPLIANCE

Technology, System and Information Integrity section requires implementation of security protection mechanisms; System and Services Acquisition section requires a properly secured infrastructure; and Configuration Management section requires the development of configuration management policies and procedures.

The Fiscal Control and Internal Auditing Act (30 ILCS 10/3001) requires the University to maintain a system, or systems, of internal fiscal and administrative controls to provide assurance that resources are utilized efficiently and effectively and in compliance with applicable law.

Finally, the University's management team is responsible for implementing timely corrective action on all of the findings identified during a State compliance examination.

University officials indicated resource constraints and competing priorities have prevented the development and adoption of formal guidelines and controls around system security.

Inadequate security controls may result in unauthorized access to, damage to, or theft of University data and computing equipment.

UNIVERSITY RESPONSE:

The University agrees with this finding and accepts the recommendation. The University currently engages in the practices listed in the recommendations but has not adopted formal policies and procedures. The University will prioritize the creation and adoption of the requisite policies and procedures before the end of Fiscal Year 2025.

UPDATED RESPONSE:

Implemented.

To address the recommendation related to physical access to computer resources, the University has implemented procedure on Data Center Access. Additionally, to address the recommendation regarding the application of vendor-released patches, procedure on Patch Management has been adopted.

15. The auditors recommend the University:

- **Establish policies and procedures to ensure performance measures are monitored to comply with contractual terms and service level agreements.**
- **Obtain and review the SOC reports of all service providers.**
- **Perform timely review of SOC reports of the service providers.**
- **Monitor and document the operation of the CUECs noted in the SOC reports that are relevant to the University's operations.**
- **Obtain and review the SOC reports of subservice providers or perform alternative procedures to determine the impact on the internal control environment of the University.**

REVIEW #4593 GOVERNORS STATE UNIVERSITY – FY24 COMPLIANCE

- **Conduct an analysis to determine the impact of noted deviations in the SOC reports to the University's internal control environment.**

FINDING: *(Inadequate Controls around Service Providers) –This finding has been repeated since 2021.*

Governors State University (University) did not have adequate controls around its service providers.

In Fiscal Year 2024, the University identified 86 service providers. The University maintains numerous cloud-based solutions with various service providers. These service providers maintain the hardware, software and data for various applications regarding many sectors, such as campus news and events, student orientation, employment, photographs, student organizations, visitor tracking, course evaluations, and emergency notifications.

During testing of 21 service providers, the auditors noted the University had not:

- Developed formal, documented policies and procedures to ensure performance measures are monitored to comply with contractual terms for the service providers tested (100%).
- Performed a review of the System and Organization Control (SOC) reports for two (10%) service providers.
- Timely reviewed the SOC reports or equivalent, for 16 (76%) service providers, with reviews conducted between 100 to 863 days after report issuance.
- Assessed and documented the operation of Complementary User Entity Controls (CUECs) relevant to the University's operations for 12 (57%) service providers.
- Obtained and reviewed SOC reports for the subservice providers or performed alternative procedures to determine the impact on the University's internal control environment for 19 (90%) service providers.
- Conducted an analysis to determine the impact of modified opinions and control deviations on 2 (50%) of 4 SOC reports.

The University is responsible for the design, implementation, and maintenance of internal controls related to information systems and operations to ensure resources and data are adequately protected from unauthorized or accidental disclosure, modifications, or destruction. This responsibility is not limited due to the process being outsourced.

Finally, this finding was first noted during the University's Fiscal Year 2021 State compliance examination. As such, University management has been unsuccessful in implementing a corrective action plan to remedy this deficiency.

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

REVIEW #4593 GOVERNORS STATE UNIVERSITY – FY24 COMPLIANCE

assurance over the entities' internal controls related to the services provided. Such assurance may be obtained via timely review of the System and Organization Control reports or independent reviews.

Further, the Fiscal Control and Internal Auditing Act (30 ILCS 10/3001) requires the University to maintain a system, or systems, of internal fiscal and administrative controls to provide assurance that resources are utilized efficiently and effectively and in compliance with applicable law.

Finally, the University's management team is responsible for implementing timely corrective action on all of the findings identified during a State compliance examination.

University officials indicated resource constraints and competing priorities have prevented full implementation of the review process including development of formal policies and procedures on ensuring due diligence on service providers and ensuring performance measures are monitored to comply with contractual terms.

Without having adequate monitoring controls over service providers, including proper and timely reviews of SOC reports or another form of independent internal control review, the University does not have assurance the service provider's internal controls are adequate to support the University's processes and ensure its data are secured.

UNIVERSITY RESPONSE:

The University agrees with this finding and accepts the recommendation. As previously noted, the University has allocated substantial resources to meet the recommendations; however, compliance is becoming more challenging as the requirements imposed upon State agencies in the pursuit of adequate third-party risk management continue to tighten. The University currently conducts a risk assessment on all known cloud service providers and assigns a risk rating based partly on the type of documentation provided by the service providers; no new contracts are signed with service providers until this review is complete. The University will continue its efforts toward compliance with the recommendations.

UPDATED RESPONSE:

Partially Implemented.

Significant progress has been made toward resolving this finding, with the review of security controls documentation and completion of risk assessments for all known third-party and subservice providers nearing 100%. Additionally, Complementary User Entity Controls (CUECs) are formally communicated to application owners, who assume responsibility for ensuring compliance.

- 16. The auditors recommend the University establish and adopt formal policies and procedures to perform and document a periodic user access review for applications.**

REVIEW #4593 GOVERNORS STATE UNIVERSITY – FY24 COMPLIANCE

Further, they recommend the University adopt formal policies on provisioning, deprovisioning, and monitoring of remote user access.

FINDING: *(Weaknesses in System Access Controls) – This finding has been repeated since 2021.*

Governors State University (University) had not established adequate controls for system access.

Upon review of the University's controls around system access, the auditors noted the University had not established and adopted formal policies and procedures for periodic review of access rights to applications to ensure appropriateness of access granted.

Additionally, they noted the University did not have formal approved policies for provisioning, deprovisioning, and monitoring of remote user access.

Finally, this finding was first noted during the University's Fiscal Year 2021 State compliance examination. As such, University management has been unsuccessful in implementing a corrective action plan to remedy this deficiency.

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, Access Control and System and Communication Protection sections, requires entities to implement adequate internal controls over access to their environments, applications and data.

The Fiscal Control and Internal Auditing Act (30 ILCS 10/3001) requires the University 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 University's resources.

Finally, the University's management team is responsible for implementing timely corrective action on all of the findings identified during a State compliance examination.

University officials indicated resource constraints and competing priorities have prevented the development and adoption of formal system access controls and procedures.

Inadequate system access and security controls may result in exposing information assets and resources to unauthorized disclosure, modification, or destruction.

UNIVERSITY RESPONSE:

The University agrees with this finding and accepts the recommendation. The University is currently building a process for periodic review of access rights to applications and plans to begin implementation shortly. Additionally, the University has formally adopted

REVIEW #4593 GOVERNORS STATE UNIVERSITY – FY24 COMPLIANCE

a procedure for provisioning, deprovisioning, and monitoring of remote user access during Fiscal Year 2025.

UPDATED RESPONSE:

Partially Implemented.

The University's Acceptable Use Policy procedure has been revised to address both recommendations. Additionally, a quarterly review process has been initiated to ensure that application owners verify user access and permissions for cloud-based applications. Full implementation across all applications is anticipated within the current fiscal year.

17. The auditors recommend the University:

- **At least annually, assess each location accepting credit card payments and match the method of acceptance to the appropriate SAQ and complete the appropriate SAQ(s) for its environment and maintain documentation.**
- **Validate merchants for all elements of its cardholder data environment verifying PCI DSS compliance.**
- **Provide annual security training to employees involved in the processing of cardholder data.**
- **Maintain an agreement with each service provider which requires the service provider to ensure validated PCI compliance for the services/solutions being provided.**

FINDING: *(Weaknesses with Payment Card Industry Data Security Standards) – This finding has been repeated since 2021.*

Governors State University (University) had not completed all requirements to demonstrate full compliance with the Payment Card Industry Data Security Standards (PCI DSS).

In Fiscal Year 2024, the University accepted approximately 18,815 credit card transactions estimated at \$15.3 million.

Upon review of the University's efforts to ensure compliance with PCI DSS, the auditors noted the University had not:

- Completed formal assessments of each merchant accepting credit card payments, including the appropriate Self-Assessment Questionnaire (SAQ) and certifying compliance;
- Validated merchants for all elements of its cardholder data environment verifying PCI-DSS compliance;
- Ensured all employees involved in the processing of cardholder data received annual security training; and

REVIEW #4593 GOVERNORS STATE UNIVERSITY – FY24 COMPLIANCE

- Maintained an agreement with each service provider which requires the service provider to ensure validated PCI compliance for the services/solutions being provided.

This finding was first noted during the University's Fiscal Year 2021 State compliance examination. As such, University management had been unsuccessful in implementing a corrective action plan to remedy this deficiency.

PCI DSS was developed to detail security requirements for entities that store, process, or transmit cardholder data. Cardholder data is any personally identifiable data associated with a cardholder. To assist merchants in the assessments of their environment, the PCI Council has established SAQ for validating compliance with PCI's core requirements. In addition, the Fiscal Control and Internal Auditing Act (30 ILCS 10/3001) requires the University to establish and maintain a system, or systems, of internal fiscal and administrative controls to provide assurance assets and resources are safeguarded against waste, loss, unauthorized use, and misappropriation.

Finally, the University's management team is responsible for implementing timely corrective action on all of the findings identified during a State compliance examination.

University officials stated resource constraints and competing priorities hindered efforts to bring University merchants into compliance with PCI DSS during Fiscal Year 2024.

Failure to complete SAQs on all merchants, and validate merchants for PCI compliance, could result in noncompliance with PCI DSS requirements or identity theft or the loss of credit card data, or loss of the right to utilize certain credit card providers if not in compliance with current PCI standards.

UNIVERSITY RESPONSE:

The University agrees with this finding and accepts the recommendation. The University continues its compliance efforts with each merchant individually, including the migration of a second merchant to a Point-to-Point Encryption solution with a third planned, easing the completion of the requisite SAQs. The University is considering options to help bring select merchants into compliance, including the possibility of engaging a third-party provider to assist with PCI-DSS compliance. In addition to mandatory annual cybersecurity awareness training, the University has established basic training for employees involved in the processing of card payments and is implementing it on a per-merchant basis.

UPDATED RESPONSE:

Partially Implemented.

Three merchants have been brought into compliance with PCI-DSS. For these merchants, employees receive annual PCI-specific security training in addition to the general cybersecurity awareness training required of all staff. Appropriate contractual language is also in place.

REVIEW #4593 GOVERNORS STATE UNIVERSITY – FY24 COMPLIANCE

Efforts are underway to bring additional merchants into compliance as resources allow. While a definitive completion date is not available, significant progress is anticipated with up to nine remaining merchants during the current fiscal year.

Emergency Purchases

The Illinois Procurement Code (30 ILCS 500/) states, “It is declared to be the policy of the state that the principles of competitive bidding and economical procurement practices shall be applicable to all purchases and contracts....” The law also recognizes that there will be emergency situations when it will be impossible to conduct bidding. It provides a general exemption when there exists a threat to public health or public safety, or when immediate expenditure is necessary for repairs to state property in order to protect against further loss of or damage to state property, to prevent or minimize serious disruption in critical state services that affect health, safety, or collection of substantial state revenues, or to ensure the integrity of state records; provided, however that the term of the emergency purchase shall not exceed 90 days. A contract may be extended beyond 90 days if the chief procurement officer determines additional time is necessary and that the contract scope and duration are limited to the emergency. Prior to the execution of the extension, the chief procurement officer must hold a public hearing and provide written justification for all emergency contracts. Members of the public may present testimony.

Notice of all emergency procurement shall be provided to the Procurement Policy Board and published in the online electronic Bulletin no later than five business days after the contract is awarded. Notice of intent to extend an emergency contract shall be provided to the Procurement Policy Board and published in the online electronic Bulletin at least 14 days before the public hearing.

A chief procurement officer making such emergency purchases is required to file a statement with the Procurement Policy Board and the Auditor General to set forth the circumstance requiring the emergency purchase. The Legislative Audit Commission receives quarterly reports of all emergency purchases from the Office of the Auditor General. The Legislative Audit Commission is directed to review the purchases and to comment on abuses of the exemption.

GSU had no emergency purchases in FY24.

Headquarters Designations

The State Finance Act requires all state agencies to make semiannual headquarters reports to the Legislative Audit Commission. Each state agency is required to file reports of all its officers and employees for whom official headquarters have been designated at any location other than that at which official duties require them to spend the largest part of their working time.

As of July 2024, GSU had 2 employees assigned to locations others than official headquarters.