LEGISLATIVE AUDIT COMMISSION

Review of
Chicago State University
620 Stratton Office Building
Springfield, Illinois 62706
217/782-7097

REVIEW: #4585
CHICAGO STATE UNIVERSITY
YEAR ENDED JUNE 30, 2024

RECOMMENDATIONS – 14

IMPLEMENTED/PARTIALLY IMPLEMENTED – 14

REPEATED RECOMMENDATIONS – 12

PRIOR AUDIT FINDINGS/RECOMMENDATIONS – 16

This review summarizes the reports on Chicago State University (CSU) for the year ended June 30, 2024. The Compliance Examination was filed with the Legislative Audit Commission on May 20, 2025. The auditors performed the audits in accordance with state law, Government Auditing Standards, the Single Audit Act and applicable federal regulations. The auditors stated that the financial statements were fairly presented.

CSU is governed by the Chicago State University Board of Trustees, which is comprised of seven members appointed by the Governor with the advice and consent of the State Senate. There is also one voting student member elected to a one-year term by the student body.

CSU's mission is to transform students' lives by innovative teaching, research and community partnership through excellence in ethical leadership, cultural enhancement, economic development and justice. CSU works toward six strategic goals as it seeks to fulfill its mission:

- Academic Excellence, Innovation and Student Transformation
- Student Enrollment, Retention and Graduation
- University Culture, Climate and Accountability
- Strengthened Infrastructure
- Cost Efficiencies and Diverse Revenue Streams
- Community Service, Urban Leadership and Economic Engagement

CSU is led by Zaldwaynaka "Z" Scott who became President on July 1, 2018. President Scott served on the CSU's Board from 2009 to 2013. She is an attorney and a former federal prosecutor and university professor as well as Illinois' first Executive Inspector General for the Agencies of the Governor and its public universities.

Appropriations and Expenditures

Appropriations ($ thousands)	FY23		FY24	
	Approp	Expend	Approp	Expend
GENERAL FUNDS				
Operational Expenses	36,769.9	36,769.9	39,343.8	39,343.8
TOTAL GENERAL FUNDS	**36,769.9**	**36,769.9**	**39,343.8**	**39,343.8**
OTHER STATE FUNDS				
Grants				
Education Improvement Fund	3,000.0	3,000.0	3,000.0	3,000.0
Pharmacy Practice Educ. & Train.	307.0	307.0	307.0	307.0
TOTAL OTHER STATE FUNDS	**3,307.0**	**3,307.0**	**3,307.0**	**3,307.0**
TOTAL	**40,076.9**	**40,076.9**	**42,650.8**	**42,650.8**

Accountants' Findings and Recommendations

Condensed below are the 14 findings and recommendations included in the audit report. Of these, 12 are repeated from the previous audit. The following recommendations are classified on the basis of information provided by the University, via electronic mail May 20, 2025.

1. 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.

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

The Chicago 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 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 testing, the auditors noted the following:

- During their testing of eligibility testing, the auditors noted 2 instructors were not reported as eligible to participate in SURS by the University. For the June 30, 2022 census data, it was determined the service credit was different by a combined total of ½ of a year. These have been previously reported but had not been corrected as of June 30, 2022.

- The University was not able to provide supporting documentation for the census data points related to 24 members selected for testing.

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.

Additionally, eligibility criteria for participation in SURS under the Illinois Pension Code (Code) (40 ILCS 5/15-134(a)) states any person who is an employee of the University becomes a participant in SURS. Under the Code (40 ILCS 5/15-107), an employee is any member of the educational, administrative, secretarial, clerical, mechanical, labor, or

other staff of an employer whose employment in a position in which services are expected to be rendered on a continuous basis for at least four months or an academic term, whichever is less:

1) not a student employed on a less than full-time temporary basis;
2) not receiving a retirement or disability annuity from SURS;
3) not on military leave;
4) not eligible to participate in the Federal Civil Service Retirement System,
5) not currently on a leave of absence without pay more than 60 days after the termination of SURS' disability benefits;
6) not paid from funds received under the Federal Comprehensive Employment and Training Act as a public service employment program participant hired on or after July 1, 1979;
7) not a patient in a hospital or home;
8) not an employee compensated solely on a fee basis where such income would net earnings from self-employment;
9) not providing military courses pursuant to a federally-funded contract where the University has filed a written notice with SURS electing to exclude these persons from the definition of an employee;
10) currently on lay-off status of not more than 120 days after the lay-off date;
11) not on an absence without pay of more than 30 days; and,
12) a nonresident alien on a visa defined under subparagraphs (F), (J), (M), or (Q) of Section 1101(a)(15) of Title 8 of the United States Code who (1) has met the Internal Revenue Service's substantial presence test and (2) became an employee on and after July 1, 1991.

In addition, the Code (40 ILCS 5/15-157) requires the University to, at a minimum, withhold contributions of each employee's total compensation of 8% (9.5% for firefighters or police officers) for their participation in SURS, unless further contributions by the employee would either exceed the maximum retirement annuity in the Code (40 ILCS 5/15-136(c)) or the Tier 2 earnings limitation within the Code (40 ILCS 5/15-111(b)), and remit these amounts to SURS. Further, the Code (40 ILCS 5/15-155(b)) requires the University to remit employer contributions to SURS reflecting the accruing normal costs of an employee paid from federal or trust funds.

Finally, for CMS' OPEB plan, the auditors noted participation in OPEB is derivative of an employee's eligibility to participate in SURS, as members of SURS participate in OPEB as annuitants under the State Employees Group Insurance Act of 1971 (Act) (5 ILCS 375/3(b)).

University management indicated the University continued to rely on manual reconciliation processes which were not fully adequate to ensure accuracy and consistency among SURS, CMS, and the records retained at the University.

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. Further, failure to report all eligible employees to SURS may result in employees not receiving the pension and OPEB benefits they are entitled to receive under the Code and the Act.

UNIVERSITY RESPONSE:
The University agrees with the recommendation. The University is developing processes to ensure all events occurring within a census data accumulation year are timely reported to SURS. Documentation and cross-training are still on-going to improve processes and minimize errors. The University will continue to review and update incremental changes to the census data file to ensure that all errors are promptly corrected.

UPDATED RESPONSE:
Recommendation accepted and partially implemented.

2. The auditors recommend the University implement adequate general IT controls related to its environment and applications.

FINDING*: Weaknesses over Computer Security – This finding has been repeated since 2020.*

The Chicago State University (University) did not maintain adequate general Information Technology (IT) controls related to its environment and applications.

The University had invested in computer hardware and systems and established several critical, confidential, or financially sensitive systems for use in meeting its mission.

Security of the environment
During testing, the auditors requested the University provide a population of its active servers. In response to this request, the University provided a listing of servers which included decommissioned servers. Due to these conditions, they were unable to conclude the University's population records were sufficiently precise and detailed under the Professional Standards promulgated by the American Institute of Certified Public Accountants (AU-C § 500.08 and AT-C § 205.36).

Despite this limitation, the auditors performed testing on a sample of servers and noted the Information Technology (IT) infrastructure was not secured properly.

Controls over access provisioning
During their testing of the University's controls over access provisioning, the auditors noted separated employees continued to have access to the University's environment.

This finding was first reported in Fiscal Year 2020. In subsequent years, the University has been unsuccessful in implementing appropriate procedures to improve its controls over computer security.

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

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 resources are utilized efficiently and effectively and in compliance with applicable law.

University management indicated the issues regarding separated employees having access to the network were due to the reliance on ad-hoc and manual processes for offboarding employees when they leave the University, resulted in delays in access revocation. University management further indicated other issues were due to the lack of monitoring technology and absence of a formal process for deprovisioning of servers.

Failure to have adequate security controls over computing resources increases the risk of unauthorized access to the computing environment and the risk that confidentiality, integrity, and availability of systems and data will be compromised.

UNIVERSITY RESPONSE:

The University agrees with the finding and acknowledges the need to strengthen controls over its IT environment and applications. To address these concerns, the University has initiated a comprehensive review of its identity and access management (IAM) processes to improve offboarding procedures and eliminate reliance on manual and ad-hoc processes. Additionally, the University is formalizing procedures for server management to ensure accurate inventory tracking and decommissioning.

As part of these efforts, the University has:

- Implemented NIST 800-171 as its governance framework to establish standardized security controls and ensure compliance with best practices.
- Been actively researching and evaluating IAM solutions that will enhance the provisioning and deprovisioning process to reduce security risks and improve efficiency.
- Worked closely with Human Resources and other key stakeholders to assess and refine existing processes, ensuring proper identity management practices while mitigating gaps in user offboarding.
- Enhanced monitoring capabilities by migrating from a mail system to a cloud service provider, which provides increased visibility into the University's technical environment. Leveraged additional security monitoring tools to improve detection, response, and overall security posture.
- Implemented IT solutions to aid in the management and monitoring of servers, improving visibility, security, and compliance with IT controls.

- Established periodic access reviews to mitigate the risk of unauthorized access.

The University remains committed to strengthening its IT controls and will continue refining its security practices to align with regulatory and industry standards.

UPDATED RESPONSE:
Recommendation accepted and partially implemented. Security monitoring tools/software to improve detection, response, and overall security posture have been implemented as well as tools/software for managing and monitoring servers.

3. The auditors recommend the University implement controls to ensure the completeness and accuracy of populations of retirees, re-employed annuitants, and employees who filed for disability benefits. Further, they recommend the University accurately report unused sick leave and timely notify re-employment of annuitants to SURS in accordance with the Code.

FINDING: *Inadequate Controls to Ensure Compliance with the Illinois Pension Code – First reported 2023, Last reported 2024*

The Chicago State University (University) did not have adequate internal controls to ensure compliance with the Illinois Pension Code (Code).

During testing, the auditors requested the University provide the populations of retired employees, persons receiving a retirement annuity (Annuitant) from the State Universities Retirement System (SURS) and re-employed by the University, and employees who filed for disability benefits during Fiscal Year 2024. The University provided the populations; however, these populations could not be reconciled to the University's internal records and SURS.

Due to this condition, the auditors were unable to conclude the University's population records were sufficiently precise and detailed under the Professional Standards promulgated by the American Institute of Certified Public Accountants (AU-C § 500.08 and AT-C § 205.36) to test the University's compliance with the Code.

Even given the population limitations noted above which hindered their ability to conclude whether selected samples were representative of the population as a whole, the auditors performed testing to determine whether the University accurately reported to SURS about unused sick leave of retired employees, certificates of disability for employees who filed for disability benefits stating the employee is unable to perform the duties, and re-employment of annuitants. During testing, they noted the following:

- Two of four (50%) retired employees' unused sick leave ranging 17 and 122 days were incorrectly reported to SURS.

- Two of two (100%) re-employed annuitants were not timely reported to SURS. The University notified SURS 9 and 347 days late.

The Code (40 ILCS 5/15-113.4) requires the University to certify to the SURS Board the number of days of unused sick leave accrued to the employee's credit on the date the employee was terminated.

In addition, the Code (40 ILCS 5/15-139.5) requires the University to notify SURS within 60 days after employing an annuitant.

Finally, 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 State's resources.

University management stated there was a significant turnover of employees within the Human Resources Department which impacted the current employees' ability to generate reports from the University's information system and timely comply with the reporting requirements of the Code.

Failure to maintain adequate internal control resulted in noncompliance with the Code and reduces the overall reliability of activity reported in the University's financial statements.

UNIVERSITY RESPONSE:
The University agrees with the recommendation and is currently working with SURS to reconcile data. Further, internal controls will be strengthened to ensure timely reporting.

UPDATED RESPONSE:
Recommendation accepted and partially implemented. Control improvements have been implemented to mitigate the risk of this finding repeating in future years.

4. The auditors recommend the University strengthen controls to ensure timely notifications are sent to students and parents upon disbursement of grant funds and loans.

FINDING: *Failure to Notify Students and Parents Upon Disbursement of Funds – This finding has been repeated since 2022.*

Federal Agency:	U.S. Department of Education
Assistance Listing Numbers:	84.379; 84.268
Program Names:	Student Financial Assistance Cluster Teacher Education Assistance for College and Higher Education Grants

	Federal Direct Student Loans
Program Expenditures:	$23,575, $17,736,297
Award Numbers:	P379T221351; P268K221351
Questioned Costs:	None

The Chicago State University (University) did not notify the students and parents upon disbursement of grant funds and loans.

Conditions Found

During testing of five students, who received Teacher Education Assistance for College and Higher Education (TEACH) Grants totaling $15,088, the auditors noted one (20%) student with a grant disbursement amounting to $3,772 was notified by the University 98 days before the TEACH funds were credited to the student's account. The sample methods used in performing this testing were not statistically valid**.**

In addition, during testing of 40 students, who received Federal Direct Loans totaling $597,967, the auditors noted the following:

- Six (15%) students with grant disbursements totaling $60,860 were not notified by the University indicating the funds were credited to the students' accounts.

- Seven (18%) students with grant disbursements totaling $44,586 were notified 35 to 120 days before or after the Federal Direct Loan funds were credited to the students' accounts.

The sample methods used in performing this testing were not statistically valid.

Evaluative Criteria

The Code of Federal Regulations (Code) (34 CFR § 668.165 (a)(3)(i)) requires the University to notify students or parents in writing no earlier than 30 days before, and no later than 30 days after, crediting the student's ledger account at the University with TEACH Grant funds and Federal Direct Loans.

Further, the Code (2 CFR § 200.303) requires the nonfederal entity receiving federal awards to establish and maintain effective internal control over the federal award to provide reasonable assurance the nonfederal entity is managing the federal award in compliance with federal statutes, regulations, and the terms and conditions of the federal award. Effective internal controls include procedures to ensure timely notification of disbursements to students receiving TEACH Grants and Federal Direct Loans.

Underlying Cause

University management indicated the failure to timely notify students and parents upon disbursements of TEACH Grants and Federal Direct Loans was due to a student aid simplification process that caused errors in financial aid processing. University management further indicated the Enterprise Resource Planning (ERP) System experienced a technical glitch during the process of sending notifications to students.

Significance
Failure to timely notify students and parents regarding grant and loan disbursements represents noncompliance with the Code.

UNIVERSITY RESPONSE:
The University agrees with the recommendation. An additional level of oversight has been added to ensure the notification of disbursement information is sent in a timely manner. The Associate Director of Financial Aid and the Director of Financial Aid will review the list of disbursements against the list of emails sent to ensure that emails are sent in a timely manner. The additional oversight will begin with the Summer 2025 disbursement based on the date of notification of the issue.

UPDATED RESPONSE:
Recommendation accepted and fully implemented. A system fix has been implemented, and all required notices have been sent for the academic year 24/25.

5. The auditors recommend the University strengthen its controls over equipment and investigate or re-examine large discrepancies identified during its annual inventory counts. In addition, they recommend the University ensure property records accurately reflect equipment on-hand, equipment items are timely inventoried, and the Certification is timely submitted to CMS in accordance with State laws and regulations. Further, the auditors recommend the University implement a formal documentation process for requesting and approving any cancellations or changes to wireless communication device services or assignments. Finally, they recommend the University establish internal controls to ensure the timely retrieval of wireless communication devices and the cancellation of telecommunication services when an employee leaves the University or upgrades their device.

FINDING*:* *Inadequate Controls over Equipment – First reported 2023, Last reported 2024*

The Chicago State University (University) did not maintain adequate controls over its equipment.

Specifically, the auditors noted the following:

- The University submitted its Annual Certification of Inventory (Certification) to the Department of Central Management Services (CMS) 229 days late.

  The Illinois Administrative Code (Code) (44 Ill. Admin. Code 5010.460) requires the University to complete and certify the University's annual physical inventory of State equipment and submit a property listing to CMS on dates designated by CMS. The University's designated due date was July 1, 2024.

- They reviewed the University's Certification submitted to the CMS. The Certification reported 352 unlocated items amounting to $748,411 or 4% of the total dollar amount of University equipment. Of the 352 unlocated equipment items:

    - 248 (70%) items consisting of iPad, laptops, uninterruptible power supply unit (UPS), and central processing units (CPUs), totaling $188,281, were missing from the Information Technology Department.

    - 11 (3%) items consisting of projector, printers, X-ray tube analyzer, television, copiers, tracking system, search device, and meter cell, totaling $188,378, were missing from the College of Pharmacy.

    - One (1%) audio visual system, totaling $120,537, was missing from the Pharmacy Practice.

    - Eight (2%) items consisting of lift tables, mega press kit, extractor, air compressor, auto scrubber, striping machine, and hydraulic bender, totaling $62,509, were missing from the Physical Facilities – Planning and Management.

    - Four (1%) items consisting of copier, CPU, and compressors, totaling $36,291, were missing from the Nursing Department.

    - 32 (9%) items consisting of laptops, CPUs, and badminton net system, totaling $21,773, were missing from the Athletics Department.

    - 48 (14%) items consisting of radio, printer, centrifuge, copiers, laptops, cash register, servers, auto scrubber, and iPad, totaling $130,642, were missing from the University Police, Property Control, Admissions, Student Affairs, Health Information Administration, Financial Aid, Library and Information Services, College of Health Sciences/Occupational Therapy, Human Resources, Psychology, Records and Registration, Educational Opportunity Center, Foreign Languages and Literature, Labor and Legal Affairs, Center for Teaching and Research Excellence, Elementary and Middle Education, Daycare Center, Office of Grants, Geography, Sociology and History Studies, Social Work, Campus Ministries, and Education Department.

  Further, the University did not investigate and/or re-examine inventory counts.

  The Code (44 Ill. Admin. Code 5010.490(f)) requires the University to conduct a re-examination and provide written explanation, and/or on-site investigations when unusually large discrepancies are identified during inventory certifications.

In addition, according to CMS annual inventory certification instructions, a loss ratio of one percent (1%) or greater of the dollar amount of inventoried items requires re-inventory of high loss ratio location codes.

Further, the University Administration and Finance Policies and Procedures Manual on Property Control Management (Policy) states each Fiscal Officer is delegated with the responsibility to retain and account for all assets under their authority. According to the Policy, each Fiscal Officer is required to know the location of all equipment assigned to their fiscal stewardship and ensure such equipment is reasonably secure from possible theft and other hazards. A physical inventory has to be conducted annually beginning March 31st in compliance with CMS rules and regulations and the Fiscal Officer is responsible for providing an explanation and supporting documentation of discrepancies identified.

- During list to floor testing, one of 25 (4%) equipment items, totaling $14,978, could not be traced to the Certification submitted to CMS. In addition, during floor to list testing, nine of 25 (36%) equipment items could not be traced to the Certification submitted to CMS and University's property records.

  The State Property Control Act (Act) (30 ILCS 605/6.02) requires each responsible officer to maintain a permanent record of all items of property under their jurisdiction and control.

  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, funds, property, and other assets and resources are safeguarded against waste, loss, unauthorized use and misappropriation, and maintain accountability over the University's resources.

- During additions testing, the auditors noted seven of 25 (28%) equipment items, totaling $45,295, were recorded in the University's property records more than 90 days after acquisition, ranging from 10 to 198 days late.

  The Code (44 Ill. Admin. Code 5010.400) requires the University to adjust property records within 90 days of acquisition, change, or deletion of equipment.

- During testing of canceled wireless communication devices, the auditors noted the University was unable to provide documentation to determine if the devices had been returned in a timely manner for three of four (75%) employees that left the University or received an upgraded device.

  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 that funds, property, and other assets and resources are safeguarded against waste, unauthorized use, and misappropriation which would include enforcing procedures to ensure

telecommunication devices are returned in a timely manner. Good internal controls over telecommunications include deactivating a wireless communication device before the end of the next billing date, if possible, to avoid unnecessary charges.

In addition, the State Records Act (5 ILCS 160/8) requires the University to make and preserve records containing adequate and proper documentation of the organization, functions, policies, decisions, procedures, and essential transactions of the University designed to furnish information to protect the legal and financial rights of the State and of persons directly affected by the University's activities.

University management indicated the issues were due to Fiscal Officer (department heads) turnover and their failure to follow the established asset management processes. In addition, the University management indicated the noted deficiency on wireless communication devices arose due to the absence of a formalized process to track and document the timely return and deactivation of wireless communication devices during employee separations or device upgrades. University management further indicated, historically, these processes were decentralized, leading to inconsistent documentation practices.

Failure to investigate or re-examine the discrepancies identified during the annual inventory and failure to exercise adequate internal controls over equipment may result in a loss of equipment due to theft and noncompliance with the State rules and regulations. In addition, failure to maintain adequate internal control over the cancellation of wireless communication devices could result in misuse of State assets and incurrence of unnecessary costs.

UNIVERSITY RESPONSE:
The University agrees with the recommendation. Internal reconciliation of equipment will be performed, and the additional oversight will begin with the Summer 2025. Further, management will implement a formal, centralized process to track the issuance, return, and cancellation of telecommunication devices.

UPDATED RESPONSE:
Recommendation accepted and partially implemented. Control improvements have been implemented at the department level. The inventory process is currently underway.

6. The auditors recommend the University strengthen controls over personal services to ensure employee timesheets, overtime timecards, and leave requests are maintained and approved by their supervisors and W-4 forms are properly maintained. In addition, they recommend the University ensure employees' gross pay rates, retirement deductions, terminated employees' lump sum payments, and accrued leave calculations are accurate. Further, the auditors recommend the University ensure employees complete the required trainings in accordance with the State Officials and Employees Ethics Act and Identity Protection Act. Lastly, they recommend University enforce monitoring procedures to ensure employee performance evaluations are timely completed.

FINDING: *Inadequate Controls over Personal Services – This finding has been repeated since 2022.*

The Chicago State University (University) did not maintain adequate controls over personal services.

- During review of 60 employees' personnel files, the auditors noted the following:
    - Five (8%) employees' gross pay rates did not agree with the established rates per the State Universities Civil Service System (SUCSS).
    - Three (5%) employees' gross pay rates could not be traced to the SUCSS; therefore, they were unable to determine if the employees' gross pay rates were in accordance with SUCSS.
    - 38 (63%) employees' W-4 forms could not be located.
    - One (2%) employee's retirement deduction was incorrectly calculated.

  The Statewide Accounting Management System (SAMS) Manual (Procedure 23.10.30) requires the agency to be responsible for completing the payroll voucher each pay period and attesting to the employee's rate of pay, gross earnings, deductions, net pay, and other required information on the voucher and file. The SAMS Manual (Procedure 23.10.30) also states that the initial control of each payroll is at the agency level.

- During testing of 60 employees' timesheets, the auditors noted the following:
    - 24 (40%) employees' timesheets could not be located; therefore, they were unable to determine if the timesheets were timely submitted and approved.
    - One (2%) employee's timesheet was approved three days late.
    - Two (3%) employees' timesheets were not approved by the employee's supervisor.

  The University's Human Resources Policy (Policy) requires managers to review the accuracy and completeness of employee time reports and approve employees' time to ensure they are recording exception time taken, and monitor and approve non-exempt employees' work time to ensure they are adhering to an approved work schedule.

- During testing of 60 employees' overtime records, the auditors noted the following:

- 28 (47%) employees' overtime timecards could not be located; therefore, they were unable to determine if overtime was properly authorized.

- 32 (53%) employees did not obtain prior authorization in order to work overtime.

- Six (10%) employees' overtime hours per timecards did not agree with University records. Specifically, they noted discrepancies ranging from eight to 56 hours.

The University's Policy states employees must receive prior authorization from their manager to work overtime. In addition, managers must keep track of the number of hours the employees work and ensure they are paid for all time worked.

The State Records Act (5 ILCS 160/8) requires the University to make and preserve records containing adequate and proper documentation of the essential transactions of the University to protect both the legal and financial rights of the State and of persons directly affected by the University's activities.

- During testing of leave of absences for five employees, the auditors noted the following:

    - One (20%) employee's leave request form was not signed by the employee's supervisor.

    - Three (60%) employees' leave request forms could not be located.

    - Two (40%) employees were overpaid, totaling $7,983, during their period of leave of absence.

  The University's Policy requires employees to submit all requests and supporting documentation for leaves of absence to the Office of Human Resources within one week of the first day of the absence.

- During review of 40 employees' accrued leave balances, auditors noted five (13%) employees' accrued leave balances were incorrectly calculated, with discrepancies ranging from 48 to 168 hours.

  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. Effective internal controls should include procedures to ensure the University accurately calculates the accrued leave balances of employees.

- During testing of 15 terminated employees, auditors noted two (13%) terminated employees' lump sum payments were incorrectly calculated, with discrepancies ranging from 288 to 383 hours.

  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. Effective internal controls should include procedures to ensure the University properly calculates the lump sum payments of terminated employees.

- During testing of 60 employees' performance evaluations, the auditors noted the following:

  - Four (7%) employees' performance evaluations were not completed.

  - Seven (12%) employees' performance evaluations were completed three to 30 days late.

  - Four (7%) employees' performance evaluations were not signed by the employees, as required.

  - One (2%) employee's performance evaluation had no indication of the completion date; therefore, they were unable to determine if the performance evaluation was completed timely.

  The University procedures require performance evaluations to be conducted annually within the due dates set forth by the University Human Resource Department or the University Faculty Personnel Action Timetable.

  In addition, the Illinois Administrative Code (Code) (80 Ill. Admin. Code 302.270) requires performance records to include an evaluation of employee performance prepared by each agency not less than annually.

- During testing of 60 employees' training requirements, the auditors noted the following:

  - One (2%) new employee did not complete the initial harassment and discrimination prevention training.
  - Two (3%) employees did not complete the annual Identity Protection Act training.
  - Four (7%) employees completed the annual Identity Protection Act training five to 32 days late.

  The State Officials and Employees Ethics Act (Act) (5 ILCS 430/5-10.5(a-5)) requires new employees to complete harassment and discrimination prevention training within 30 days after beginning of employment. The Act also requires each

officer, member, and employee to complete, at least annually, a harassment and discrimination prevention training program.

Additionally, the Identity Protection Act (5 ILCS 179/37) requires all employees identified as having access to social security numbers in the course of performing their duties to be trained to protect the confidentiality of social security numbers. The training should include instructions on handling of information that contains social security numbers from the time of collection through destruction of the information.

This finding was first reported during the year ended June 30, 2022. In the subsequent years, the University has been unsuccessful in implementing appropriate corrective action.

University management indicated, as they did in prior examination, the exceptions noted were due to staffing constraints.

The review and approval of employee timesheets, overtime timecards, and leave requests is a systematic and uniform approach to ensure no employee is misreporting their time spent on official University business. In addition, failure to approve and maintain timesheets, overtime cards, and W-4 forms, along with failure to accurately calculate lump sum payments for terminated employees and the appropriate retirement deductions, as well as ensuring the gross pay rates align with SUCSS may result in incorrect compensation for services rendered and results in noncompliance with University policies and State statutes. Failure to complete the harassment and discrimination training may result in employees not recognizing harassment or discrimination and understanding their rights and responsibilities under the Act. Failure to complete the Identity Protection Act training may result in employees mishandling information containing social security numbers. Finally, performance evaluations are a systematic and uniform approach used for the development of employees and communication of performance expectations to employees. Failure to conduct timely employee performance evaluations delays formal feedback on an employee's performance, areas for improvement, and the next year's performance goals and objectives. In addition, employee performance evaluations should serve as a foundation for salary adjustments, promotions, demotions, discharge, layoff, recall, or reinstatement decisions.

UNIVERSITY RESPONSE:

The University agrees with the recommendations and will work to implement controls over payroll and leave processes, required training, and completion of performance evaluations.

UPDATED RESPONSE:

Recommendation accepted and partially implemented. HR is coordinating efforts with Payroll to improve internal controls in personal services processes. Additionally, new technology solutions are being evaluated to automate monitoring of performance evaluations.

7. The auditors recommend the University maintain a complete and accurate list of contractual agreements. In addition, they recommend the University establish appropriate procedures to ensure all contracts are signed and executed prior to the commencement of services. Further, they recommend the University review its procedures to ensure exempt purchases are timely published in the Illinois Procurement Bulletin.

FINDING: *Inadequate Controls over Contractual Services Expenditures – This finding has been repeated since 2016.*

The Chicago State University (University) did not have adequate controls over contractual services expenditures.

During their testing of contractual agreements, the auditors requested the University to provide the population of contractual agreements including interagency agreements entered into during the examination period. In response to this request, the University provided a listing of purchase orders issued during the examination period. However, upon checking the completeness and accuracy of the listing provided, they noted the following:

- The University did not maintain an up-to-date list of new and existing contracts effective for the examination period.

- Multiple purchase orders can be linked to a single contract. Therefore, a single purchase order does not necessarily indicate a new contract. As such, they were unable to determine the completeness of new contracts based on the purchase order listing.

In addition, the University was unable to provide a listing of interagency agreements.

Due to these conditions, auditors were unable to conclude the University's population records were sufficiently precise and detailed under the Professional Standards promulgated by the American Institute of Certified Public Accountants (AT-C § 205.36).

Even given the population limitations noted above which hindered the ability of the accountants to conclude whether selected samples were representative of the population as a whole, they obtained the available population provided by the University, selected a sample, and tested for compliance. During our review of 33 contracts (totaling $3,127,481), including purchase orders, executed during the fiscal year ended June 30, 2024, they noted the following:

- Four contracts (totaling $218,817) were executed subsequent to the start date of the contracts. The contract execution dates ranged from 7 to 89 days from the commencement of services.

- Three exempt purchases (totaling $742,949) were not published in the Illinois Procurement Bulletin, while three exempt purchases (totaling $346,441) were published 14 to 89 days late.

- One contract amounting to $23,400 was not approved by the authorized staff.

This finding was first reported during the year ended June 30, 2016. In subsequent years, the University has been unsuccessful in implementing appropriate corrective action.

The State Records Act (5 ILCS 160/8) requires the University to make and preserve records containing adequate and proper documentation of the essential transactions of the University to protect both the legal and financial rights of the State and of persons directly affected by the University's activities.

In addition, the Illinois Procurement Code (Code) (30 ILCS 500 et seq.) and the Statewide Accounting Management System (Procedure 15.20 et seq.) require contracts to contain certain signatures of authorized representatives and disclosures. Moreover, the Code (30 ILCS 500/1-13) requires notices of exempt purchases to be published in the Procurement Bulletin within 14 calendar days after contract execution. Additionally, the Code (30 ILCS 500/20-80(d)) requires that contractors are not to be paid for any supplies that were received or services that were rendered before the contract was reduced to writing and signed by all necessary parties.

Lastly, 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. Effective controls should include procedures to ensure contracts are properly approved, published, and fully executed prior to performance.

University management indicated the exceptions were due to inadequate controls and lack of timely action of concerned staff.

Failure to maintain a complete and accurate listing of contractual agreements may result in expenditures not being timely encumbered and paid. In addition, failure to fully execute a contract prior to the commencement of services leaves the University vulnerable to unnecessary liabilities and potential legal issues. Furthermore, failure to publish contracts in the Illinois Procurement Bulletin and include all appropriate approval signatures result in noncompliance with the University procurement policies and procedures, and State statutes and regulations.

UNIVERSITY RESPONSE:

The University agrees with the recommendation. A contract management software would be deployed in Fiscal Year 2026, which will provide contract repository, visibility, contract creation/authoring, contract performance management, and other features to improve contract efficiency at the University.

UPDATED RESPONSE:
Recommendation accepted and partially implemented. A new Procurement Director was appointed as well as additional staff. Technology solutions are planned for 2Q2026. Outreach and training are extended to departments to help ensure compliance. Additionally, control improvements to ensure proper documentation of exception justifications has been implemented and is working as intended.

8. The auditors recommend the University prepare and timely file the Agency Workforce Report with the Office of the Governor and Secretary of State.

FINDING: *Failure to Prepare and File the Agency Workforce Report – First reported 2023, Last reported 2024*

The Chicago State University (University) did not prepare and file its Agency Workforce Report (Report) for Fiscal Year 2023 with the Office of the Governor and Secretary of State.

The State Employment Records Act (Act) (5 ILCS 410/20) requires the University to prepare the Agency Workforce Report on a fiscal year basis and file the Report by January 1 each year with the Office of the Governor and Secretary of State.

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. Effective controls should include procedures to ensure Reports are timely filed with the Office of the Governor and Secretary of State.

University management indicated the failure to file the Agency Workforce Report was due to staffing constraints.

Failure to prepare and file the Report with the Office of the Governor and Secretary of State resulted in noncompliance with the Act.

UNIVERSITY RESPONSE:
The University agrees with the recommendation and will prepare and timely file the Agency Workforce Report by January 1 of each year with the Office of the Governor and Secretary of State. The most recent report has been submitted timely.

UPDATED RESPONSE:
Recommendation accepted and fully implemented. Control improvements have been implemented, and the most recent report has been filed timely.

9. The auditors recommend the University:

- **Obtain and review SOC reports to ensure the service providers' internal controls are adequate.**

- **Review SOC reports and monitor and document the operation of CUECs relevant to the University's operations.**

- **Obtain and review SOC reports for subservice providers or perform alternative procedures to determine the impact on the University's internal control environment.**

- **Document the deviations noted in the SOC reports and perform an analysis of the impact of those deviations on the University's internal control environment.**

FINDING: *Lack of Adequate Controls over Review of Internal Controls over Service Providers – This finding has been repeated since 2020.*

The Chicago State University (University) did not have adequate internal controls over its service providers.

The University entered into agreements with various service providers to assist in some of its needed processes to operate effectively and efficiently such as: (1) payment system for receipts and expenditures, (2) purchasing system, (3) processing payments to Perkins's student loans, and (4) tracking of University property and equipment.

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

- Obtained and reviewed the System and Organization Controls (SOC) reports for one (25%) service provider.

- Monitored and documented the operation of the Complementary User Entity Controls (CUECs) relevant to the University's operations identified in the SOC reports for one (25%) service provider.

- Obtained and reviewed SOC reports of the subservice organizations or performed alternative procedures to determine the impact of the subservice organizations on the University's internal control for one (25%) service provider.

- Conducted an analysis to determine the impact of noted deviations within the SOC report on the University's internal control for one (25%) service provider.

This finding was first reported in Fiscal Year 2020. In subsequent years, the University has been unsuccessful in implementing appropriate procedures to improve its controls over service providers.

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

In addition, 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 administrative controls, to provide assurance revenues, expenditures, and transfers of assets, resources, or funds applicable to operations are properly recorded and accounted for to permit the preparation of accounts and reliable financial and statistical reports to maintain accountability over the State's resources. Strong management controls, due diligence, and fiduciary responsibility require adequate supervision of service providers.

University management stated decentralized vendor management and resource constraints contributed to gaps in service provider monitoring.

Failure to consider the application of CUECs to the University and perform additional assessments on the subservice providers lessens the effectiveness of reliance on the SOC reports as an element of internal control structure. Additionally, failure to obtain and review SOC Reports of service and subservice organizations will not provide assurance the service and subservice providers' internal controls are adequate. Finally, failure to conduct an analysis to determine the impact of deficiencies in the service provider's control environment could impact the University's internal controls.

ACCOUNTANT'S COMMENTS:

The University agrees with the recommendation and is formalizing procedures to obtain, review, and document SOC reports for all relevant service providers and their subservice organizations. The University will evaluate CUECs, track any deviations, and assess their impact on the internal control environment. These actions will enhance oversight and align with the Fiscal Control and Internal Auditing Act.

UPDATED RESPONSE:

Recommendation accepted and partially implemented. Control improvements, including a centralized third-party risk management process and coordination with other units, have been implemented to mitigate the risk of this finding repeating in future years.

10. The auditors recommend the University reconcile the Fiscal Year 2023 census data, submit the required certifications along with any potential errors noted to SURS, and work with SURS to address any errors noted.

FINDING: *Census Data Reconciliation – New*

The Chicago State University (University) did not complete its annual census data reconciliation and certification.

During their testing, the auditors noted the University did not reconcile changes in the State Universities Retirement System (SURS) member data to University records or submitted the required census data reconciliation certification for FY23 data, as required by SURS, by May 30, 2024, although they had a process in place to do so.

In accordance with the American Institute of Certified Public Accountants' (AICPA's) Audit and Accounting Guide: State and Local Governments, SURS requires each university to reconcile the employee census data annually to a report provided by SURS' actuary. This reconciliation process helps mitigate the risk of using incomplete or inaccurate data and ensures the accuracy of reported pension and other post-employment benefit (OPEB) balances. Further, this reconciliation process ensures the completeness of employer and plan data, reduces payroll errors, confirms personnel files are up-to-date, and most importantly decreases the risks of financial misstatements. SURS requested the University to reconcile their Fiscal Year 2023 census data, certify to SURS that the reconciliation was completed, and report any potential data errors found by May 30, 2024.

University management indicated the failure to submit census data certification was due to staffing constraints.

Failure to perform reconciliations and submit certifications could lead to reduced reliability of pension and OPEB related information and balances.

UNIVERSITY RESPONSE:
The University agrees with the recommendation and will reconcile the census data and work with SURS to address any errors noted.

UPDATED RESPONSE:
Recommendation accepted and partially implemented. A new benefits manager has been hired, trained, and is currently working with SURS to complete the reconciliation process.

11. The auditors recommend the University:

- **Ensure staff and contractors acknowledge their understanding of the University's information security policies and procedures.**
- **Perform a comprehensive risk assessment to identify and ensure adequate protection of confidential or personal information.**
- **Classify its data to ensure adequate protection.**

- **Formalize, approve, and implement the standard operating procedures over existing security solutions to provide effective security and resilience of assets.**

- **Ensure adequate implementation and documentation of information security incident response procedures.**

- **Ensure all employees and contractors complete security awareness trainings**.

FINDING: *Weaknesses in Cybersecurity Programs and Practices – This finding has been repeated since 2020.*

The Chicago State University (University) did not maintain adequate internal controls related to its cybersecurity programs and practices.

Given the University's responsibilities, it maintains a substantial amount of personal and confidential information, including Social Security numbers, addresses, and educational records.

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 their examination of the University's cybersecurity program, practices, and control of confidential information, the auditors noted the University had not:

- Ensured staff and contractors acknowledged their understanding of the University's information security policies and procedures.

- Performed a comprehensive risk assessment to identify and ensure adequate protection of confidential or personal information.

- Classified its data to ensure adequate protection.

- Formalized its standard operating procedures over existing security solutions to provide effective security and resilience of assets.

- Ensured adequate implementation and documentation of information security incident response procedures.

In addition, two of 60 (3%) employees had not completed security awareness training. Furthermore, contractors were not required to complete cybersecurity training.

This finding was first reported in Fiscal Year 2020. In subsequent years, the University has been unsuccessful in establishing adequate controls related to cybersecurity programs and practices.

The *Framework for Improving Critical Infrastructure Cybersecurity* and *Security and Privacy Controls for Information Systems and Organizations* (Special Publication 800-53, Fifth Revision) published by the National Institute of Standards and Technology require 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 to maintain accountability over the State's resources.

Additionally, the University's Security and Awareness Training Policy requires all University staff and employees with access to IT systems to review and sign the IT Division's Acceptable Use Agreement, acknowledging understanding of security responsibilities and best practices to safeguard university's data.

Further, the University's Security Incident Response Policy (Policy) requires all staff and employees to promptly report any actual or suspected security incidents. The Policy requires the incidents to be documented, evidence preserved, and analysis activities conducted.

University management stated manual tracking, gaps in University practices, competing IT priorities, and staffing shortages have led to compliance discrepancies.

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

UNIVERSITY RESPONSE:

The University agrees with the recommendation and has initiated efforts to strengthen the University's cybersecurity program. These efforts include formalizing standard operating procedures for existing security tools, conducting a comprehensive risk assessment, implementing data classification, and improving documentation for incident response. The University will also reinforce policy acknowledgment processes and ensure all employees and contractors complete required security awareness training. These actions will improve compliance with internal policies and the Fiscal Control and Internal Auditing Act.

UPDATED RESPONSE:

Recommendation accepted and partially implemented. Updated policies and coordinated with Human Resources to ensure security training for all employees.

12. The auditors recommend the University update the Plan to depict the current environment along with detailed recovery steps. They also recommend the University perform a disaster recovery testing at least annually.

FINDING: *Inadequate Disaster Recovery Process – This finding has been repeated since 2020.*

The Chicago State University's (University) did not ensure an adequately updated and tested disaster recovery plan exists to ensure timely recovery of critical computer systems.

The University had a disaster recovery plan (Plan) to guide the University in the recovery of its computing and network facilities in the event of a disaster. However, the Plan was not revised since 2016, and it did not depict the current environment and did not contain detailed steps to recover its environment, applications, and data. Additionally, the disaster recovery testing was not performed since 2018.

This finding was first reported in Fiscal Year 2020. In subsequent years, the University has been unsuccessful in establishing adequate controls related to its disaster recovery.

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), Contingency Plan section, requires reviewing the contingency plan and updating the plan to address the changes to the organization, system, environment of operation and problems encountered during contingency plan implementation, execution, or testing. NIST also requires testing of the Plan to determine the effectiveness and readiness to execute the recovery procedures.

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.

University management indicated the University has not conducted formal disaster recovery (DR) testing during the current audit period due to the lack of a fully developed and regularly updated disaster recovery policy and testing framework. University management further indicated the University has not yet established a consistent and documented testing process to validate system recovery effectiveness. Additionally, University management indicated competing institutional priorities and limited funding have delayed the formalization of disaster recovery policies and procedures, as well as the execution of full-scale disaster recovery exercises.

Failure to have an adequately updated and tested disaster recovery plan leaves the University exposed to the possibility of major disruptions to services.

UNIVERSITY RESPONSE:

The University agrees with the recommendation and is actively updating the University's disaster recovery plan to reflect the current environment, systems, and recovery procedures. The University is also developing a documented testing framework and plans to conduct a disaster recovery exercise in the upcoming fiscal year. These efforts will align with NIST 800-53 requirements and strengthen compliance with the Fiscal Control and Internal Auditing Act.

UPDATED RESPONSE:
Recommendation accepted and partially implemented. Disaster Recovery policy is being updated to align with current NIST standards. A risk-based testing schedule will be established.

13. They auditors recommend the University complete the appropriate SAQ(s) and AOC and maintain documentation supporting its validation efforts.

FINDING: *Weaknesses with Payment Card Industry Data Security Standards – New*

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

The University accepted credit card payments for tuition, student fees, and parking fees. In Fiscal Year 2024, the University handled approximately 12,000 credit card transactions totaling approximately $1.8 million.

The auditors reviewed the efforts of the University to ensure compliance with PCI DSS. During their testing, they noted the University had not completed appropriate Self-Assessment Questionnaires (SAQ) and Attestation of Compliance (AOC) for its programs accepting credit card payments.

To assist merchants in the assessments of their environment, the PCI Council has established SAQs for validating compliance with PCI's core requirements. At a minimum, PCI DSS required completion of SAQ A and associated AOC; which highlights specific requirements to restrict access to paper and electronic media containing cardholder data, destruction of such media when it is no longer needed, and requirements for managing service providers.

University management indicated the issues noted were due to oversight.

The lack of validation of controls over credit card payments increases the risk of unauthorized disclosure of cardholder data.

UNIVERSITY RESPONSE:

The University agrees with the recommendation and Student Financial Services will complete the respective SAQ(s) documentation supporting credit card payment transactions both in-person and online.

UPDATED RESPONSE:
Recommendation accepted and partially implemented. Coordination with internal units has been formalized to ensure compliance with deadlines, required submissions, and ongoing monitoring. Extended training is also planned.

14. The auditors recommend the University strengthen controls to ensure I-9 Forms are properly completed, reviewed, and maintained in accordance with the Code.

FINDING: *Weaknesses over Maintenance of Employment Eligibility Verification Forms – This finding has been repeated since 2022.*

The Chicago State University (University) did not ensure the U.S. Citizenship and Immigration Services (USCIS) Employment Eligibility Verification forms (I-9 Form) were properly maintained.

During testing of 60 employees, the auditors noted the following:

- Fourteen (23%) employees did not have the completed I-9 Forms on file. As such they could not determine if the University examined the identity and employment authorizations of these employees.

  The Code of Federal Regulation (Code) (8 CFR § 274a.2(a)(3)) requires an employer to examine documents that evidence the identity and employment authorization of the individual. The employer must complete an attestation on the I-9 Form under penalty of perjury.

  Moreover, the Code (8 CFR § 274a.2(b)) requires an employer to retain a paper (with original handwritten signatures), electronic, or a combination of paper and electronic formats of I-9 Forms, three years after the date of the hire or one year after the date the individual's employment is terminated, whichever is later.

- One (2%) I-9 Form had Section 1, Employee Information and Attestation, completed and signed by the employee 21 days late and had Section 2, Employer Review and Verification, completed and signed by the University's authorized representative 12 days late.

  The Code (8 CFR § 274a.2(b)(i)(A)) requires the employee to complete Section 1 of I-9 Form at the time of hire and sign the attestation with a handwritten or electronic signature. In addition, the Code (8 CFR § 274a.2(b)(ii)(B)) requires the employer to review and verify Section 2 of I-9 Form within three business days of

the hire and sign the attestation with a handwritten signature or electronic signature.

This finding was first reported during the year ended June 30, 2022. In subsequent years, the University has been unsuccessful in implementing appropriate corrective action.

The Fiscal Control and Internal Auditing Act (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 resources are utilized efficiently, effectively, and in compliance with applicable law. Effective internal controls should include procedures to ensure I-9 Forms are completed and retained.

University management indicated the exceptions on I-9 Forms were due to staff turnover and staffing constraints.

Failure to complete and retain I-9 Forms is a violation of the Code and could result in unlawful employment and expose the University to penalties.

UNIVERSITY RESPONSE:
The University agrees with the recommendation and will implement controls to ensure I-9 Forms are properly completed, reviewed, and maintained.

UPDATED RESPONSE:
Recommendation accepted and implemented.

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.

In the first quarter of FY24, CSU had one emergency purchase for an estimated cost of $631,500 in other funds to provide food service to support students, staff, and faculty.

In the third quarter of FY24, CSU had one emergency purchase for an estimated cost of $651,500 in other funds to provide food service to support students, staff, and faculty.

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 2, 2024, the University had 5 employees assigned to locations others than official headquarters.