LEGISLATIVE
AUDIT
COMMISSION

Review of
Illinois State University
For the Year Ended June 30, 2023

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

REVIEW: #4578
ILLINOIS STATE UNIVERSITY
YEAR ENDED JUNE 30, 2023

FINDINGS/RECOMMENDATIONS – 11

IMPLEMENTED/PARTIALLY IMPLEMENTED – 9
ACCEPTED – 0
UNDER STUDY - 2

REPEATED RECOMMENDATIONS – 7

PRIOR AUDIT FINDINGS/RECOMMENDATIONS – 11

This review summarizes the auditors' reports on the compliance examination of the Illinois State University for year ended June 30, 2023, filed with the Legislative Audit Commission on May 2, 2024. The reports were conducted in accordance with *Government Auditing Standards* and State law. The auditors' stated the University's financial statements were presented fairly.

Illinois State University is a residential university with seven colleges and 36 academic departments that offer more than 170 programs of study. The Graduate School coordinates 61 masters', specialist, and doctoral programs. Illinois State University is located in Normal, IL and governed by the Board of Trustees. It was founded in 1857 and is the oldest public institution of higher learning in Illinois.

Dr. Aondover Tarhulé was appointed interim president on February 17, 2023, following the resignation of Dr. Terri Goss Kinzy. Dr. Tarhulé was named president on March 18, 2024. Prior to being appointed interim president, Dr. Tarhulé served as vice president for academic affairs and provost as well as serving as a professor in the Department of Geography, Geology, and the Environment.

Appropriations and Expenditures

	FY22		FY23	
Appropriations ($ thousands)	**Approp**	**Expend**	**Approp**	**Expend**
GENERAL FUNDS				
Operational Expenses	73,100.3	73,100.3	73,100.3	73,100.3
TOTAL GENERAL FUNDS	**73,100.3**	**73,100.3**	**73,100.3**	**73,100.3**
OTHER STATE FUNDS				
Grants				
Scholarship Grant Awards	25.0	21.9	25.0	25.0
TOTAL OTHER STATE FUNDS	**25.0**	**21.9**	**25.0**	**25.0**
TOTAL	**73,125.3**	**73,122.2**	**73,125.3**	**73,125.3**

Accountants' Findings and Recommendations

Condensed below are the 11 findings and recommendations included in the audit report. Of these, seven are repeated from the previous audit. The following recommendations are classified on the basis of information provided by Illinois State University, via electronic mail received May 2, 2024.

1. The auditors recommend the University implement adequate security, including:

- **Approving the updated policies and procedures to (1) reflect the University's current environment and (2) address future changes in processes and new systems; and**
- **Documenting, during formal user access reviews, the appropriateness of each user's access to the University's applications for all departments;**

Additionally, auditors recommend the University strengthen its controls to maintain a complete and accurate population of servers, update their servers with the vendors' latest versions of antivirus and operating systems, conduct security assessments over its environment, and ensure all security operations are properly configured.

FINDING: *(Information Security Weaknesses) – First Reported 2018, Last 2023*

The Illinois State University (University) had multiple computer security weaknesses.

The University relies on its computing environment for maintaining several critical, sensitive, and/or confidential systems used to meet its mission.

During testing of university information technology controls, auditors noted the University:

- Had not developed access provisioning policies documenting the internal controls for all environments and applications.
- Had not developed a policy documenting requirement for an annual review of users' access.
- Had not conducted a review of users' access.
- Had not developed a policy documenting the review of security violation reports to ensure remediation is timely conducted.

In order to determine if proper security controls had been implemented across the University's environment, auditors requested a population of servers. Although the University provided a population, documentation demonstrating its completeness and accuracy was not provided. Due to these conditions, auditors were unable to conclude the Office's population records were sufficiently precise and detailed under the Professional Standards promulgated by the American Institute of Certified Public

Accountants (AU-C § 330, AT-C § 205). Even given the population limitations, they tested the population of servers, noting the University could not provide documentation demonstrating the antivirus and operating system were running the vendors' latest versions.

In addition, the auditors testing noted the University had not:

- Conducted security assessments over its environment.
- Ensured all security operations were properly configured.

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

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

University officials indicated the IT functions and resources are highly distributed across the institution which require considerably more time to change and improve. University officials also indicated IT is limited in capacity to fully organize the remediation efforts within the portfolio of work efforts required of IT across the institution.

Inadequate controls over changes to the University's environment, applications and data could lead to unauthorized access, unauthorized changes and security risks to its environments, applications and related data. Also, due to the severity of the weaknesses noted, the auditors were unable to rely upon the general IT controls over the environments and applications.

UNIVERSITY RESPONSE:

The University agrees and understands that many of the issues identified are localized to specific departments rather than systemic across the organization. In response, we are committed to developing a comprehensive corrective action plan that addresses each identified issue promptly and effectively. This plan will include targeted strategies for the departments in question, ensuring that we uphold the highest standards of operation and security consistently across their institution.

UPDATED RESPONSE:

Partially Implemented.

The University is working through the shared governance process to finalize, communicate, and effectuate relevant policy, procedures, and standards to ensure consistent application of the Information Security Program across the institution.

2. The auditors recommend the University implement controls to maintain a list of all of their service providers and determine and document if a review of the service providers' internal controls were performed, if required.

Additionally, auditors recommend the University:

- **Obtain SOC reports or perform independent reviews of internal controls for all service providers.**
- **Monitor and document the operation of the CUECs relevant to the University's operations.**
- **Either obtain and review SOC reports for subservice organizations or perform alternative procedures to satisfy itself that the existence of the subservice organization would not impact its internal control environment.**
- **Document its review of the SOC reports and review all significant issues with subservice organizations to ascertain if a corrective action plan exists and when it will be implemented, any impacts to the University, and any compensating controls.**

<u>FINDING:</u> *(Lack of Adequate Controls over the Review of Internal Controls over Service Providers) – New*

The Illinois State University (University) did not implement adequate internal controls over its service providers.

The auditors requested the University provide a population of their service providers utilized in order to determine if the University had reviewed the internal controls of its service providers. However, the University was not able to provide such a population. Additionally, auditors noted the University had not developed policies and procedures to ensure their due diligence and monitoring of their service providers. Furthermore, the University did not obtain System and Organization Control (SOC) reports to ensure the internal controls at the service providers had been implemented and were operating effectively.

Due to these conditions, auditors were unable to determine if the internal controls of the service providers were adequate, and they were required to perform alternative procedures.

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

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

University officials indicated that the various functions for holistic service provider management are distributed across various departments without a unifying strategy at this time.

Without having obtained and reviewed SOC reports or another form of independent internal control review, the University does not have assurance the service providers' internal controls are adequate and operating effectively.

UNIVERSITY RESPONSE:

The University agrees and understands that while our procedures and practices are effective in their defined scope, there is a need for formalized institution-wide policy to ensure consistency in all environments. In response, we are committed to developing a comprehensive corrective action plan that results in the development and implementation of change management governance.

UPDATED RESPONSE:

Partially Implemented.

The University is in the process of reviewing and assessing its processes to formalize an institution-wide policy/procedures to ensure consistency across campus and develop an approach for risk-based management of service providers.

3. **The auditors recommend the University implement adequate policies and procedures over changes to the University's environment, applications and data. They also recommend the University maintain documentation that changes are properly approved prior to implementation.**

   Further, auditors recommend the University strengthen its controls in maintaining a population of system developers and individuals with administrative rights.

FINDING: *(Weaknesses in Change Control) – New*

The Illinois State University (University) did not maintain adequate internal controls over changes to its environment, applications and data.

The University had not developed a change management policy documenting the internal controls over changes to its environment, applications and data. In addition, the University had not implemented a formal Change Management Board.

Further, the approval for changes, including emergency changes, prior to being implemented into production was not maintained.

Lastly, the University was unable to provide documentation demonstrating the population of system developers and individuals with administrative rights was complete and accurate. Due to these conditions, 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 § 330, AT-C § 205). Even given the noted limitations, they tested the system developers and individuals with administrative rights, noting no exceptions.

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), Configuration Management section, require entities to maintain proper internal controls over the changes to the environment, applications and data.

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

University officials indicated the lack of recent review and assessment of change management procedures and practices resulted in the noted gaps developing.

Inadequate controls over changes to the University's environment, applications and data could lead to unauthorized access, unauthorized changes and security risks to its environments, applications and related data. Also, due to the severity of the weaknesses noted, auditors were unable to rely upon the general IT control over the environments and applications.

UNIVERSITY RESPONSE:

The University agrees and understands that while our procedures and practices are effective in their defined scope, there is a need for formalized institution-wide policy to ensure consistency in all environments. In response, we are committed to developing a comprehensive corrective action plan that results in the development and implementation of change management governance.

UPDATED RESPONSE:

Partially Implemented.

The University is in the process of reviewing and assessing existing distributed change management processes to develop centralized oversight to ensure institutional goals are supported and process gaps are adequately addressed.

4. The auditors recommend the University review its current process for preparing the SEFA and implement the necessary procedures to ensure the SEFA is prepared timely and accurately in accordance with the Uniform Guidance.

FINDING: *(Inaccurate Reporting of Federal Expenditures on the Schedule of Expenditures of Federal Awards) – New*

Condition: Illinois State University (University) did not have an adequate process in place to prepare and review its Schedule of Expenditures of Federal Awards (SEFA), prior to providing it to the auditors.

The University provided us their final SEFA on September 27, 2023. On February 27, 2024, the University informed us their SEFA did not include ten federal programs with expenditures during the fiscal year totaling $3,556,085.

Criteria: According to 2 CFR 200.510(b), a recipient of Federal awards is required to prepare a SEFA for the period covered by the entity's financial statement which must include the total Federal awards expended. At a minimum, the schedule must include (1) a list of individual Federal programs by Federal agency. For a cluster of programs, provide the cluster name, list individual Federal programs within the cluster of programs and provide the applicable Federal agency name; (2) for Federal awards received as a subrecipient, the name of the pass-through entity and identifying number assigned by the pass-through entity must be included; (3) provide total Federal awards expended for each individual Federal program and the Assistance Listings Number or other identifying number when the Assistance Listings Number is not available; (4) include the total amount provided to subrecipient from each Federal program; and (5) include notes that describe the significant accounting policies used in preparing the schedule.

In addition, 2 CFR 200.303 requires non-Federal entities to, among other things, establish and maintain effective internal control over the Federal award that provides reasonable assurance that the non-Federal entity is managing the federal award in compliance with Federal statutes, regulations, and the terms and conditions of the Federal award. Effective internal controls should include procedures to ensure expenditures are properly reported on the schedule of expenditures of Federal awards.

Cause: University officials indicated the review process in place did catch the missing items, however not prior to providing the SEFA to the auditors for their testing.

Effect: Failure to accurately and timely report federal expenditures on the SEFA could result in the auditors not being able to properly determine the major programs that would be required to be audited in accordance with the Uniform Guidance and resulted in noncompliance with federal regulations.

UNIVERSITY RESPONSE:
The University agrees with the finding. The University will revise the timing of internal reviews to provide an accurate final SEFA to auditors in a timely manner. All agreements, including intergovernmental agreements and federal contracts for services will be included in the institutional reports used to construct the schedule to aid in timely reporting.

UPDATED RESPONSE:
Implemented.
The Schedule of Expenditures of Federal Awards will be completed based on an agreed upon time frame to provide appropriate review time prior to providing to the external auditors.

5. **The auditors recommend the University:**
    - **Develop policies regarding configuration management, system development, training, onboarding, and backup verification and offsite storage.**
    - **Conduct security awareness training.**
    - **Conduct a comprehensive risk assessment and implement risk reducing controls.**
    - **Review the Appropriate Use Policy and the Data Classification Policy at least annually.**
    - **Classify their data in accordance with the data classification methodology.**
    - **Document the security solutions utilized to monitor the security of their assets.**
    - **Develop a comprehensive cybersecurity plan.**
    - **Strengthen controls to identify the population of vulnerabilities**.

FINDING: *(Weakness in Cybersecurity Programs and Practices) – First Reported 2019, Last 2023*

The Illinois State University (University) had not implemented adequate internal controls related to cybersecurity programs and practices and control of confidential information.

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

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

- Developed policies regarding configuration management, system development, training, on-boarding, and backup verification and offsite storage.
- Formally reviewed the Policy on Appropriate Use of Information Technology Resources and Systems (Appropriate Use Policy) since 2011.
- Conducted security awareness training.
- Conducted a comprehensive risk assessment or implemented risk reducing controls within the examination period.
- Reviewed their Data Classification Policy since 2015.
- Classified their data in accordance with the data classification methodology.
- Documented the security solutions utilized to monitor the security of their assets.
- Developed a comprehensive cybersecurity plan.

It was also noted the University could not provide a population of vulnerabilities identified during the examination period.

This finding was first identified in the June 30, 2019, Compliance Examination. Since then, the University has not implemented corrective actions.

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

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

University officials indicated other competing priorities hindered the ability of the University's IT personnel to address the weaknesses.

The lack of an adequate cybersecurity program and adequate cybersecurity practices could result in unidentified risks and vulnerabilities, which could ultimately lead to the University's confidential and personal information being susceptible to cyberattacks and unauthorized disclosure.

UNIVERSITY RESPONSE:

The University acknowledges the statements on weaknesses, cause, and potential risks as detailed in this finding. The University agrees that the statements are accurate and relevant for the period reviewed.

The University acknowledges the dynamic challenges posed by the rapidly evolving field of cybersecurity. Historically, new issues have been identified in this section each year. In response, the University remains committed to addressing these vulnerabilities and implementing the recommendations. Our approach prioritizes the most significant and effective improvements that can be made within our resource constraints, ensuring that we continually enhance our cybersecurity posture.

The University has nearly completed a comprehensive assessment of its information technology and security policies, including those specific to cybersecurity. This review involved a detailed inventory and analysis of existing policies to determine the necessity of updates or the development of new policies. The findings from this assessment revealed that, although our current practices and procedures effectively fulfill our mission objectives, the lack of formally documented policies presents a risk to consistent adherence. We are now focused on formalizing these policies to mitigate this risk and ensure sustained compliance.

In response to the audit, the University has updated its 2022 information security awareness training program and is actively disseminating it across the campus community. We are also enhancing the methods used to communicate and distribute this training to ensure comprehensive access, especially outside of conventional delivery methods. These improvements are designed to increase engagement and completion rates, reinforcing our commitment to security awareness at all levels.

The University has adopted the Center for Internet Security (CIS) Risk Assessment Methodology (RAM) for conducting thorough information risk assessments. We have focused initial assessments on mission-critical systems and areas handling highly sensitive data. This structured approach allows for periodic reassessment against the CIS Controls framework which is specifically tailored to combat the most significant and likely threats facing our information assets.

The University continues to strategically allocate its limited resources towards the most crucial and effective security initiatives, including the implementation and optimization of active safeguards. While detailed, context-specific documentation is undoubtedly beneficial, we currently rely on solution-embedded documentation to guide our practices. As more resources become available, we are committed to enhancing our documentation efforts to better support our security measures and operational needs.

Responses to Specific Sub-Findings

- Develop policies regarding configuration management, system development, training, onboarding, and backup verification and offsite storage.

Our current practices and procedures effectively fulfill the cyber security objectives, but the lack of documented policies poses a risk. The university will create a plan to mitigate this risk.

- Conduct security awareness training.

  The University has made considerable progress in security training but acknowledges that further improvements will be needed.

- Conduct a comprehensive risk assessment and implement risk reducing controls.

  The University has an information risk management plan and continues to make progress in this area and acknowledges that further improvements will be needed.

- Review the Appropriate Use Policy and the Data Classification Policy at least annually.

  The University has begun the process of updating the Appropriate Use Policy. The university will create a plan to review the Data Classification Policy. The university acknowledges that these policies must be reviewed annually.

- Classify their data in accordance with the data classification methodology.

  The University acknowledges that practices in this area should follow the policy and will create a plan to meet this objective.

- Document the security solutions utilized to monitor the security of their assets.

  The University has made considerable progress adopting modern security solutions and acknowledges that these need to be documented.

- Develop a comprehensive cybersecurity plan.

  The University has made considerable progress in this area. It has developed and adopted a comprehensive, nationally recognized cybersecurity plan that meets its objectives. The University is open to suggestions on how to improve its plan and will seek external expert advice.

- Strengthen controls to identify the population of vulnerabilities.

  The University has made considerable progress in this area. It acknowledges that growing threats requires strengthening these controls and believes that its current cybersecurity plan meets this need.

UPDATED RESPONSE:
Partially Implemented.
The University is working through the shared governance process to finalize, communicate, and effectuate relevant policy, procedures, and standards to ensure consistent application of the Information Security Program across the institution. While

treated as a separate and distinct scope, the University manages cybersecurity as a part of its Information Security Program.

6. **The auditors recommend the University continue working on establishing adequate and tested contingency plans to ensure all critical operations can be recovered within the required timeframe. At a minimum, the plans should reflect the current environment, identify a prioritized list of critical applications and minimum recovery times, outline recovery team responsibilities and contact information, and discuss alternative recovery locations and off-site storage facilities.**

   In addition, they recommend the plan be tested annually and updated where necessary based upon the test results.

FINDING: *(Inadequate Business Continuity and Disaster Recovery Planning) – First Reported 2019, Last 2023*

The Illinois State University (University) needs to improve its business continuity and disaster recovery planning process.
The University relies on its computing environment for maintaining several critical, financially sensitive, and/or confidential systems used to meet the University's needs.
During testing, auditors noted:

- The University's business continuity plan did not define specific departmental procedures, recovery point objectives, and recovery time objectives. Additionally, the University had not conducted testing of the business continuity plan.
- The University did not ensure all administrative units had developed and tested contingency plans.

This finding was first identified in the June 30, 2019, Compliance Examination. Since then, the University has not implemented corrective actions.

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 administration controls to provide assurance that University property and resources are safeguarded against waste, loss, unauthorized use, and misappropriation. Further 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 Planning section, requires entities to develop and document a business continuity plan addressing roles, responsibilities, and coordination among entities, keeping the plan up to date, and testing the plan.

University officials indicated given both the University's decentralized structure where various units across the campus establish their individual business continuity and disaster recovery plans with the coordination of these plans into one overall plan set by the University's Emergency Management Department and the shared governance process, additional time and resources will be needed to correct these long-standing problems.

Inadequate disaster recovery practices could result in the University not being able to timely recovery its environment, applications, and data.

UNIVERSITY RESPONSE:

The University acknowledges this finding. In June 2022, the President's Cabinet approved a proposal to create a university-wide continuity of operations program. Since then, staff have been surveying a field of software and implementation partners, identifying pilot departments, and working with IT to schedule and prioritize this initiative. Upon implementation, every University department will have an approved continuity plan, at which point the effort moves into operations which includes periodic plan reviews, testing, and activation, when needed.

UPDATED RESPONSE:

Partially Implemented.

The University has contracted with a firm to provide continuity software and professional services. The University identified departments, programs, and centers that will develop continuity plans and launched a multi-year continuity program by convening a steering team. Departments, programs, and centers will be engaged in the Fall 2024 to begin formal continuity planning.

7. **The auditors recommend the University run the IIEE or seek legislative remedy with CSU to formally transfer the IIEE to CSU.**

FINDING: *(Failure to Run the Illinois Institute for Entrepreneurship Education) – First Reported 2021, Last 2023*

The Illinois State University (University) did not run the Illinois Institute for Entrepreneurship Education (IIEE).

During testing, auditors noted that University transferred the IIEE to the Chicago State University (CSU) during Fiscal Year 2011.

The Illinois State University Law (110 ILCS 675/20-115) requires the University run the IIEE to "foster the growth and development of entrepreneurship education in the State of Illinois" and to "help remedy the deficiencies in the preparation of entrepreneurship education teachers, increase the quality and quantity of entrepreneurship education programs, improve instructional materials, and prepare personnel to serve as leaders and consultants in the field of entrepreneurship education and economic development."

The University came to an agreement with CSU to develop and plan the IIEE. To date, the Board of Trustees of the University and the Board of Trustees of CSU have been unable to enact a change in legislation to reflect this change in responsibility.

Failure to run the IIEE limits the ability of the University's students who become teachers from learning about the entrepreneurship education, limits the ability of those teachers to teach their future students about entrepreneurship, and represents noncompliance with State law.

UNIVERSITY RESPONSE:
The University acknowledges the finding and will continue to seek legislative support to eliminate this law.

UPDATED RESPONSE:
Under Study.
The University is seeking legislative support to eliminate this law.

8. **The auditors recommend the University implement controls to provide assurance employees timely complete training in accordance with applicable State law and retain evidence of their completion of mandated training events.**

FINDING: *(Inadequate Control over Training) – First Reported 2019, Last 2023*

The Illinois State University (University) did not consistently ensure its employees completed statutory training requirements.

During testing of 40 employees, auditors noted 2 (5%) employees with access to social security numbers (SSNs) in the normal course of their employment lacked documentation to substantiate they had completed training on how to protect SSNs during the current fiscal year.

In addition, they noted 2 of 40 (5%) new hires within the employee sample completed their initial ethics training and sexual harassment prevention training between four to five days late.

The Identity Protection Act (5 ILCS 179/37) requires the University to adopt policies requiring University employees with access to SSNs receive training on the proper handling of SSNs from the time of collection through destruction. University Policy 1.13, which was adopted on November 9, 2009, mandates University employees required to use or handle SSNs be trained on "proper procedures for handling information containing SSNs from the time of collection through the destruction of the information, in order to protect the confidentiality of SSNs."

Further, the State Records Act (5 ILCS 160/8) requires the University to make and preserve records containing adequate and proper documentation of the functions and transactions of the University to protect the legal rights of the State and of persons directly impacted by the University's activities.

University officials indicated due to turnover; the University's IT management group that was to oversee the training of department security liaisons did not properly identify that security liaisons were not identified for training.

The State Officials and Employee Ethics Act (Act) (5 ILCS 430/5-10(c)) requires new employees complete their initial ethics training within 30 days after commencing employment. Further, the Act (5 ILCS 430/5-10.5(a)) requires new employees complete their initial sexual harassment prevention training within 30 days after commencing employment.

University officials stated the one exception noted for Ethics training was an extra-help employee and the failure to complete the training was due to employee oversight.

Further, 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.

Good internal controls over compliance include establishing and maintaining a system, or systems, of internal administrative controls to provide assurance the University's operations comply with applicable laws, rules, and regulations.

Failure to ensure records of employee training are created and retained hinders the accountability and limits the ability of the University to substantiate compliance with State law. Further, failure to ensure employees timely complete ethics and sexual harassment prevention training represents noncompliance with the Act, may hinder efforts to increase awareness of ethics laws and sexual harassment prevention, and could result in employees being unaware of their responsibilities.

UNIVERSITY RESPONSE:

The University acknowledges the finding.

Regarding the SSN data protection training, the University acknowledges the statements on weaknesses, cause, and potential risks as detailed in this finding. The University agrees that the statements are accurate and relevant for the period reviewed. The University has since conducted an internal audit on SSN data use across the institution which identified key improvements to existing processes. The improvements are currently under consideration by the Data Governance Committee for prioritization and implementation.

The University trains over 6,400 employees annually and 2,400 employees as new hires each year for the Ethics and Sexual Harassment Prevention training, across all employee classifications. The one exception noted was an extra-help employee (part-time/seasonal). In an effort to maintain an effective and efficient training system, the University utilizes an online learning management system to train employees for both the annual and new hire training. The University works to ensure employees complete the required training courses. Employees and their supervisors are sent weekly e-mail reminders for those employees that have not completed their required training. The University has procedures and controls in place to train employees and maintain an effective and efficient training system in compliance with applicable requirements and will continue to work to ensure employees are trained timely and in compliance with applicable training requirements.

UPDATED RESPONSE:
Implemented.
The University continues to train employees and works to maintain and make improvements to an effective and efficient training system to ensure employees are trained timely and in compliance with applicable training requirements.

9. The auditors recommend the University's Provost take appropriate corrective action and implement internal controls to ensure faculty members with outside research, consulting services, or employment receive written pre-approval to conduct the requested activity and annually disclose the time spent on these activities in accordance with State law and University policy.

FINDING: *(Noncompliance with the University Faculty Research and Consulting Act) – First Reported 2012, Last 2023*

The Illinois State University (University) did not always ensure compliance with the University Faculty Research and Consulting Act and University policies regarding outside employment.

During Fiscal Year 2023, faculty members reported 105 instances of outside employment to the University Provost.

During testing, the auditors noted the following:

- 26 of 66 (39%) instances had the Request for Approval of Secondary/ Outside Employment Form (Form PERS 927) submitted by the faculty member for approval by the University's Provost between 1 to 189 days late.
- 38 of 66 (58%) instances had Form PERS 927 approved by the University's Provost between 1 to 498 days late.
- 23 of 66 (35%) instances did not have the Annual Report of Secondary/Outside Employment (PERS 928) submitted by the faculty member.
- 3 of 66 (5%) instances had the Form 928 submitted by the faculty member to the University's Provost approved between 6 to 60 days late.

- 1 of 66 (2%) instances had the Form 928 submitted by the faculty member to the University's Provost, however it was not approved.

Further, this finding was first noted during the University's Fiscal Year 2012 State compliance examination. As such University management has been unsuccessful in implementing a corrective action plan to remedy these deficiencies.

The Act (110 ILCS 100/1) prohibits full-time University faculty members from undertaking, contracting for, or accepting anything of value in return for research or consulting services for any person other than the University unless the faculty member:

1) has submitted a request to the University President, or designee, which includes an estimate of the amount of time involved;
2) received the prior written approval of the University President, or designee, to perform the outside research or consulting services; and,
3) submits to the University President, or designee, an annual statement of the amount of time actually spent on outside research or consulting services.

The University President has designated the University's Provost as his designee for approvals and recordkeeping.

In accordance with University Policy 3.3.7, all forms of secondary/outside employment by a faculty member require the prior written approval of the faculty member's department chairperson, dean, and the University Provost before the faculty member can accept outside employment. Further, the instructions for the Form PERS 928 require faculty members with secondary/outside employment submit the Form PERS 928 "no later than August 31 of the following fiscal year for timely routing to the Office of the Provost."

In addition, good internal controls over compliance include establishing and maintaining a system, or systems, of internal administrative controls to provide assurance the University's operations comply with applicable laws, rules, and regulations.

University officials indicated, as they did during prior year, these conditions were due to employee errors and oversight.

Failure to ensure faculty members with outside research, consulting services, or employment obtain written pre-approval from the University's Provost and file annual reports with the University's Provost about the amount of time spent during the preceding fiscal year on outside research, consulting services, or employment represents noncompliance with State law and University Policy 3.3.7 and hinders the oversight of outside activities by the University as intended by the General Assembly.

UNIVERSITY RESPONSE:

The University acknowledges the finding. The University continues to inform faculty of the reporting obligation as well as evaluation and review of the process to improve compliance.

UPDATED RESPONSE:
Partially Implemented.
The University continues to evaluate and make improvements to the process. The University's policies and processes are under review to improve the process and compliance.

10. The auditors recommend the University revise its policy and require all employees submit time sheets in compliance with State law.

FINDING: *(Noncompliance with the State Officials and Employees Ethics Act) – First Reported 2005, Last 2023*

The Illinois State University (University) did not require positive time reporting for all employees in compliance with the State Officials and Employees Ethics Act (Act).

During testing, auditors noted University Policy 1.12 only requires positive time reporting for the University's non-faculty employees. The faculty and graduate students within academic positions, academic/professional employees, and some civil service employees do not report actual hours worked and are only required to report benefit usage time (vacation, sick, etc.) used to the nearest quarter hour.

Further, this finding was first noted during the University's Fiscal Year 2005 State compliance examination. As such, University management has been unsuccessful in implementing a corrective action plan to remedy this deficiency.

The Act requires the Board of Higher Education (Board), 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 time sheets documenting the time spent each day on official State business to the nearest quarter hour." The Board adopted personnel policies for public universities on February 3, 2004, in accordance with the Act. The University has not fully incorporated these policies into the University's policies.

In addition, good internal controls over compliance include establishing and maintaining a system, or systems of internal administrative controls to provide assurance the University's operations comply with applicable laws, rules, and regulations.

University officials stated, as they did in prior years, that the University continues to work with the faculty to bring the University into compliance with the Act.

By not requiring time sheets from all of its employees, the University does not have complete documentation of time spent by employees on official State business as contemplated by the Act.

UNIVERSITY RESPONSE:
The University acknowledges the finding and will continue to work towards a feasible solution to incorporate compliance.

UPDATED RESPONSE:
Under Study.
The University continues to work towards a feasible solution to ensure compliance with this Act.

11. **The auditors recommend the University review its voucher processing function to identify and mitigate processing areas or steps causing delays in the University's approval and payment process. In addition, the University should ensure all travel vouchers are promptly submitted by its travelers in strict adherence with Publication 535, or allocate income to the traveler under a nonaccountable plan.**

FINDING: *(Inadequate Control over Voucher Processing) – New*

The Illinois State University (University) did not have adequate internal control over its voucher processing function.

During testing of 166 vouchers, totaling $13,954,618, auditors noted fourteen (8%) vouchers tested, totaling $735,471, were approved for payment between 35 and 103 days after the University received the voucher's related invoice.

During testing of 40 travel vouchers, totaling $18,453, auditors noted one (3%) tested voucher, totaling $157, was submitted by the traveler 48 days after the last day travel occurred without providing a reasonable cause for the delay.

Good internal controls over compliance include approving or denying, in whole or in part, a vendor's invoice within 30 days after receiving an invoice and then paying the approved portion of an invoice within 90 days after receiving the invoice.

Internal Revenue Service (IRS) Publication 535, Business Expenses, notes employees receiving travel reimbursements must have paid or incurred deductible expenses while performing employment services, adequately accounted for the expenses within a reasonable period of time, generally defined by Publication 535 as within 60 days after the expenses were paid or incurred, and returned any excess reimbursements within a reasonable period of time. If the employee meets all three tests, the employee is under an accountable plan and the reimbursements are not included as on the employee's Form W-2. If the employee fails any of these tests, the employee is under a nonaccountable plan and all amounts paid as travel reimbursements are reported as wages on the employee's Form W-2, subject to income, Social Security, Medicare, and unemployment taxes.

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

In addition, good internal controls over compliance include establishing and maintaining a system, or systems, of internal administrative controls to provide assurance the University's operations comply with applicable laws, rules, and regulations.

University officials indicated these exceptions were due to processing delays attributable to staffing levels and required training.

Failure to establish and maintain adequate internal control over voucher processing increases the likelihood errors or other irregularities could occur and not be detected in a timely manner by employees in the normal course of performing their assigned duties, increases the risk liabilities and expenses could be misstated on the University's financial statements, and could result in vendor dissatisfaction. Further, failure to require the timely submission of travel vouchers could result in additional efforts by the University's staff to allocate income to employees who are subject to a nonaccountable plan and represents noncompliance with IRS Publication 535.

UNIVERSITY RESPONSE:
The University acknowledges the finding. The University acknowledges that additional staff training is needed related to prompt processing of invoices. The University will provide training, reinforcing the need for identifying when invoices are received to ensure invoices are approved for payment within 30 days.

UPDATED RESPONSE:
Implemented.
The University continues to provide training related to timely submission of invoices. Invoice processing/approval processes have been updated to provide timelier submissions for processing.

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.

The University had no emergency purchases in FY23. However, in the 2nd quarter of FY25, the University has an estimated $33 million emergency purchase to redevelop a property into a new ISU College of Engineering Facility.

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 2023, Illinois State University had 226 employees assigned to locations others than official headquarters.