STATE OF ILLINOIS
OFFICE OF THE
AUDITOR GENERAL
Frank J. Mautino, Auditor General

SUMMARY REPORT DIGEST

NORTHEASTERN ILLINOIS UNIVERSITY

State Compliance Examination
For the Year Ended June 30, 2023

Release Date: May 23, 2024

FINDINGS THIS AUDIT: 13			
	New	Repeat	Total
Category 1:	0	3	3
Category 2:	4	6	10
Category 3:	0	0	0
TOTAL	4	9	13
FINDINGS LAST AUDIT: 12			

AGING SCHEDULE OF REPEATED FINDINGS			
Repeated Since	Category 1	Category 2	Category 3
2022	23-02, 23-03		
2020	23-01	23-07	
2019		23-04, 23-08	
2018		23-12, 23-13	
2017		23-05	

INTRODUCTION

This digest covers the Northeastern Illinois University (University) Compliance Examination for the year ended June 30, 2023. Separate digests covering the University's Financial Audit and Single Audit as of and for the year ended June 30, 2023 were previously released on March 28, 2024. In total, this report contains 13 findings, 7 of which were reported in the Financial Audit and Single Audit collectively.

SYNOPSIS

- **(23-08)** The University did not maintain adequate internal controls related to its cybersecurity programs and practices.
- **(23-10)** The University did not comply with the Campus Security Enhancement Act of 2008.
- **(23-12)** The University did not have adequate controls over its property and equipment.

Category 1: Findings that are **material weaknesses** in internal control and/or a **qualification** on compliance with State laws and regulations (material noncompliance).

Category 2: Findings that are **significant deficiencies** in internal control and **noncompliance** with State laws and regulations.

Category 3: Findings that have **no internal control issues but are in noncompliance** with State laws and regulations.

FINDINGS, CONCLUSIONS, AND RECOMMENDATIONS

Weaknesses in Cybersecurity Programs and Practices

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

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

The Illinois State Auditing Act (30 ILCS 5/3-2.4) requires the Auditor General to review State agencies and their cybersecurity programs and practices. During our examination of the University's cybersecurity program, practices and control of confidential information, we noted:

University lacked documented on-boarding policy or HR Manual for University contractors

- The University does not have a documented on-boarding policy or Human Resource (HR) Manual for University contractors that outlines policies, procedures, guidelines, and rules governing various aspects of contractual obligations within the University.
- Cybersecurity policy reviews are captured when a revision is made to the University's policies. However, evidence of reviews that do not result in revisions do not appear to be documented.

Specific control actives were not identified for each evaluated category

- Specific control activities were not identified for each of the categories evaluated in the Risk Register and Risk Assessment.
- There was no documented evidence that the provided reports were complete or accurate related to listings of new employees and contractors hired.
- 1 of 13 (8%) new employees tested and 1 of 7 (14%) new contractors tested with access to the University's system(s) did not complete cybersecurity training and did not acknowledge the University's policies.

This finding was first reported in Fiscal Year 2019. In subsequent years, the University has been unsuccessful in establishing adequate controls related to cybersecurity. (Finding 08, pages 25-26). **This findings has been reported since 2019.**

We recommended the University:

- Modify all onboarding and HR Manuals to include contractors.
- Update policies for review dates in addition to revised dates.

- Further develop the risk register and risk assessment to ensure specific control activities are thoroughly documented.
- Document evidence employee listing are complete and accurate.
- Ensure annual cybersecurity training and acknowledgement of policies is completed and acknowledged by all employees and contractors.

University agreed with auditors

The University agreed with the recommendation.

NONCOMPLIANCE WITH THE CAMPUS SECURITY ENHANCEMENT ACT OF 2008

The University did not comply with the Campus Security Enhancement Act of 2008 (Act).

In our testing of 7 employees in security-sensitive positions we noted:

Employees in security-sensitive positions did not complete background investigation timely or at all.

- One (14%) employee did not have a criminal background investigation completed until over 19 months after their hire date.
- One (14%) employee did not have a criminal background investigation completed. (Finding 10, page 29)

We recommended the University complete criminal background investigations for their employees in security sensitive positions prior to the beginning of their employment. In addition, we recommended the University complete criminal background investigations for all employees in security-sensitive positions for which a prior background check was not obtained.

University agreed with auditors

The University agreed with the recommendation.

INADEQUATE CONTROLS OVER UNIVERSITY PROPERTY AND EQUIPMENT

The University did not have adequate controls over its property and equipment.

During our testing of 25 equipment additions totaling $189,449, we noted the following:

Equipment additions were not timely recorded in the University's property records or in the correct fiscal year

- 12 (48%) additions tested were not recorded in the University's property records within 90 days of acquisition.
- 5 (20%) assets purchased and received during 2023 were entered into the fixed asset system as 2024 additions.

During the inventory observation, 1 of 6 (17%) items observed for testing, a projector, could not be located within the inventory listing.

Auditors noted weakness over University's annual inventory count

The University did not have approved written policies and procedures on certain critical functions and processes related to equipment management such as:

- Proper conduct of the physical count process including the objective of the count, timing and types of counts, instructions for counting and recording, and researching and adjusting discrepancies, as well as procedures and trainings to new employees to perform the count.
- Delineating the categories of equipment that are subject to theft with value less than the nominal value to ensure equipment is marked with a unique identification number. Without a policy addressing the accountability and control of high theft equipment items, there is an increased risk of University property loss without timely detection. (Finding 12, pages 31-32) **This finding has been reported since 2018.**

We recommended the University improve its procedures to ensure equipment records are accurately maintained and assets are properly accounted for. We also recommended the University establish relevant equipment management policies to ensure procedures are observed consistently by employees.

University agreed with auditors

The University agreed with the recommendation.

OTHER FINDINGS

The remaining findings are reportedly being given attention by the University. We will review the University's progress towards the implementation of our recommendations in our next State compliance examination.

AUDITOR'S OPINIONS

The financial audit was previously released. Our auditors stated the financial statements of the University as of and for the year ended June 30, 2023 are fairly stated in all material respects.

The single audit was previously released. Our auditors conducted a Single Audit of the University as required by the Uniform Guidance and stated the University complied, in all material respects, with the types of compliance requirements that could have a direct and material effect on the University's major federal programs for the year ended June 30, 2023.

ACCOUNTANT'S OPINION

The accountants conducted a State compliance examination of the University for the year ended June 30, 2023, as required by the Illinois State Auditing Act. The accountants qualified their report on State compliance for Findings 2023-001, 2023-002, and 2023-003. Except for the noncompliance described in these findings, the accountants stated the University complied, in all material respects, with the requirements described in the report.

This State compliance examination was conducted by Plante & Moran, PLLC.

SIGNED ORIGINAL ON FILE

JANE CLARK
Division Director

This report is transmitted in accordance with Section 3-14 of the Illinois State Auditing Act.

SIGNED ORIGINAL ON FILE

FRANK J. MAUTINO
Auditor General

FJM:JGR