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

SUMMARY REPORT DIGEST

STATE UNIVERSITIES RETIREMENT SYSTEM

Compliance Examination
For the Year Ended June 30, 2021

Release Date: March 10, 2022

FINDINGS THIS AUDIT: 2			
	New	Repeat	Total
Category 1:	0	0	0
Category 2:	2	0	2
Category 3:	0	0	0
TOTAL	2	0	2
FINDINGS LAST AUDIT: 1			

AGING SCHEDULE OF REPEATED FINDINGS			
Repeated Since	Category 1	Category 2	Category 3
No Repeat Findings			

INTRODUCTION

This digest covers our compliance examination of the State Universities Retirement System (System) for the year ended June 30, 2021. A separate Financial Audit as of and for the year ended June 30, 2021, was previously released on December 22, 2021.

SYNOPSIS

- (**21-1**) The System had not implemented formal internal controls related to cybersecurity programs, practices and control of confidential information.

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.

STATE UNIVERSITIES RETIREMENT SYSTEM
COMPLIANCE EXAMINATION
For the Year Ended June 30, 2021

FINANCIAL OPERATIONS	2021	2020*
Additions		
Contributions		
Participants	$ 387,003,295	$ 375,425,229
Employer	2,063,056,696	1,917,039,188
Total Contributions	2,450,059,991	2,292,464,417
Investment Income		
Net appreciation (depreciation) in fair market value	4,487,065,768	216,995,420
Interest	199,329,911	191,342,519
Dividends	187,253,566	200,038,867
Securities lending	6,340,430	5,597,401
Less: Investment expense	(86,733,426)	(68,471,370)
Net Investment Income	4,793,256,249	545,502,837
Total Additions	7,243,316,240	2,837,967,254
Deductions		
Benefits	2,782,740,275	2,677,989,974
Refund of contributions	79,128,037	69,001,514
Contributions sent to third-party administrator	178,536,338	170,278,264
Administrative expense	21,966,859	19,234,313
Total Deductions	3,062,371,509	2,936,504,065
Net Increase	$ 4,180,944,731	$ (98,536,811)
* FY20 information was restated for the adoption of GASB 84		

INVESTMENTS USED FOR BENEFITS AND EXPENSES (Defined Benefit Plan)(Unaudited)	JUNE 30, 2021	JUNE 30, 2020
Contributions		
Participants	$ 288,476,321	$ 282,367,290
State of Illinois	1,921,742,123	1,785,817,785
Federal/Trust and other sources	57,001,310	52,968,295
Total Contributions	2,267,219,754	2,121,153,370
Deductions		
Benefits	2,780,374,481	2,676,192,703
Refunds	79,128,037	69,001,514
Administrative Expenses	19,389,167	18,469,275
Total Deductions	2,878,891,685	2,763,663,492
Investments Used to Pay Benefits and Expenses	$ (611,671,931)	$ (642,510,122)

SUPPLEMENTARY INFORMATION	JUNE 30, 2021	JUNE 30, 2020
Asset management expenses	$ 86,162,787	$ 67,967,190
Investment return	23.8%	2.6%
Average number of employees (Unaudited)	162	157
Number of active members	73,443	76,335
Number of inactive members	96,753	94,024
Number of retirement benefit recipients (Unaudited)	59,872	59,060
Number of survivor benefit recipients (Unaudited)	9,332	9,157
Number of disabilities benefit recipients (Unaudited)	544	583
Number of disabilities retirement allowance recipients (Unaudited)	363	372

EXECUTIVE DIRECTOR

During Audit Period: Martin Noven (through 2-19-21), Acting - Suzanne Mayer (effective 2-20-21)
Current: Suzanne Mayer (effective 12-9-21)

FINDINGS, CONCLUSIONS, AND RECOMMENDATIONS

Lack of Cybersecurity Programs and Practices

The State Universities Retirement System (System) had not implemented formal internal controls related to cybersecurity programs, practices and control of confidential information.

It is the mission of the System to "secure and deliver retirement benefits promised" to its members. As a result, the System maintains large volumes of confidential information including retiree names, addresses, health information, Social Security numbers, bank account numbers, etc.

The Illinois State Auditing Act (30 ILCS 5/3-24) requires the Auditor General to review State agencies and their cybersecurity programs and practices. During our examination of the System's cybersecurity program, practices, and control of confidential information, we noted the System had not:

- Developed a configuration management policy, system development standards, and onboarding procedures for contractors.

- Developed policies and procedures for reviewing and monitoring security implementation and violations.

Policies and procedures had not been reviewed since 2017

- Periodically reviewed its policies and procedures to ensure they depicted the current security environment. The last review was conducted in 2017.

- Developed a project management framework to ensure new applications were adequately developed and implemented in accordance with management's expectations.

Comprehensive risk assessment not conducted

- Developed a risk management methodology, conducted a comprehensive risk assessment, or implemented risk reducing internal controls.

- Required employees to acknowledge receipt of changes to the System's policies.

Data had not been classified

- Developed a data classification methodology and classified its data to identify and ensure adequate protection of information.

- Required contractors to complete cybersecurity training.

- Conducted a review of individuals with physical access to the System's offices.

- Implemented tools to actively monitor security events over all their applications.

Although the System had developed a change management policy, it did not address control over emergency changes, approval to move changes to the production environment, and proper segregation of duties. (Finding 1, pages 8-11).

We recommended the System:

- Develop policies regarding configuration management, system development, and onboarding for contractors.
- Develop policies and procedures for reviewing and monitoring security implementation and violations.
- At least annually review its policies and procedures to ensure they depict the current security environment.
- Develop a project management framework to ensure new applications are adequately developed and implemented.
- Develop a risk management methodology, conduct a comprehensive risk assessment, and implement risk reducing internal controls.
- Require employees to acknowledge receipt of changes to the System's policies.
- Develop a data classification methodology and classify its data to identify and ensure adequate protection of information.
- Require contractors to complete cybersecurity training.
- Conduct a review of individuals with physical access to the System's offices.
- Implement tools to actively monitor security events over all their applications.

Additionally, we recommended the System update its change management policy to include control related to:

- Emergency changes,
- Approvals to move changes to the production environment, and
- Proper segregation of duties.

System response

System officials disagreed with the statement "The State Universities Retirement System had not implemented formal internal controls related to cybersecurity programs, practices and control of confidential information." SURS maintains a highly secure computer environment that safeguards confidential and personal information from attacks and unauthorized disclosure, but it recognizes that formal policies and procedures need to be documented to show how this is being done. SURS hired an Information Security Manager at

the beginning of fiscal year 2022, to assist with formalizing and developing new policies, procedures, and strengthening controls around information security.

In addition to the new position, SURS began a formal Policy Program Management Project to organize current policies and procedures and to develop a standardized process for drafting, reviewing, and approving current and new policies. Although this project is still on-going, once completed it will include a full repository of all SURS policies (including a Policy on Policies) and a process to ensure that the review and approval of each new policy and subsequent policy modification is documented. SURS is also developing a formal process to be used when employees are required to sign an acknowledgement that they have reviewed and are aware of the policies that are applicable to them.

The Configuration and Change Management policies have been updated to reflect the recommendations above. The System Development Lifecycle policy documentation will be reviewed and updated. Procedures already exist in SURS service desk for onboarding contractors. SURS will review these procedures and update if necessary.

SURS already has solutions in place for monitoring security events and automated response solutions and already subscribes to third party solutions to assist with 24 x 7 monitoring and remediation of critical events. SURS recognizes the importance of centralizing events from all applications and systems into a central solution to provide visibility and response automation and will investigate commercial solutions available. Once these tools have been identified and implemented, new policies and procedures will be developed to reflect the current policies and procedures in place.

The Project Management Office is new to SURS and is still being developed. SURS concurs with the recommendation that there is a need to implement a project management framework to ensure new applications are adequately developed and implemented.

SURS performs an annual formal risk assessment of its information and technology systems to identify current and future risk, and to identify and implement controls that mitigate that risk. With the onboarding of the Security Manager, SURS will address the need to formalize the policies and procedures in the area of Risk Management that are already in place.

During fiscal year 2020, SURS contracted with a third-party vendor to assist with a data classification methodology which has been implemented. A policy was also developed through this process, however, has not yet been formally

approved and adopted. This policy will be formally approved as part of the Policy Program Management Project.

SURS currently offers cybersecurity training to all contract workers and to all vendors who have access to our network as part of the Pension Administration System Project, however, SURS does not currently mandate that the contract workers complete cybersecurity training. SURS will work with contract workers, contractors and vendors that have access to the SURS system to ensure that they have completed cyber security awareness training on at least an annual basis. Regarding new contracts moving forward, it should be noted that absent a specific law that requires these contractors and vendors to complete cyber security awareness training on an annual basis as a condition precedent of doing business with SURS, we may not be able to obtain these recommended contract terms.

SURS conducts periodic reviews of building access to sensitive areas but does not currently perform an annual review of all facility access. SURS will create procedures to perform this review.

Accountant's Comment

In an Accountant's Comment we noted that Cybersecurity programs and practices entails more than ensuring the entities environment is secure. A Cybersecurity program also requires formally documented and adequately detailed policies, procedures, training and monitoring for security events. As documented above, the System had not formally developed or implemented such controls.

Further, a Cybersecurity program necessitates the completion of a comprehensive risk assessment which includes identifying the applications and confidential data in order to map the controls to safeguard the integrity, security and availability of the applications and data. The System had not conducted such an assessment.

OTHER FINDING

The remaining finding pertains to a Lack of Formal Controls over the Review of Internal Controls for Service Providers. We will review the Agency's progress towards the implementation of our recommendations in our next State compliance examination.

AUDITOR'S OPINION

The auditors stated the financial statements of the System as of and for the year ended June 30, 2021 are fairly stated in all material respects.

ACCOUNTANT'S OPINION

The accountants conducted a compliance examination of the System for the year ended June 30, 2021, as required by the Illinois State Auditing Act. The accountants stated the System complied, in all material respects, with the requirements described in the report.

This compliance examination was conducted by BKD, LLP.

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:TLK