

STATE OF ILLINOIS
ILLINOIS STATE UNIVERSITY

Report Required under *Government Auditing Standards*
For the Year Ended June 30, 2020
Performed as Special Assistant Auditors
for the Auditor General, State of Illinois

**State of Illinois
Illinois State University**

**Financial Audit
For the Year Ended June 30, 2020**

Table of Contents

	<u>Page(s)</u>
University Officials	1
Government Auditing Standards Report	
Summary	2 - 3
Independent Auditor's Report on Internal Control Over Financial Reporting and on Compliance and Other Matters Based on an Audit of Financial Statements Performed in Accordance with <i>Government Auditing Standards</i>	4 - 5
Schedule of Findings	
Current Findings	6 - 15

Other Reports Issued Under a Separate Cover

The Illinois State University's *Compliance Examination* (including the Single Audit) for the year ended June 30, 2020, will be issued under a separate cover. Additionally, the University's financial statements as of and for the year ended June 30, 2020, have been issued under a separate cover.

**State of Illinois
Illinois State University**

**Financial Audit
For the Year Ended June 30, 2020**

University Officials

President	Dr. Larry Dietz
Vice President for Finance and Planning	Mr. Dan Stephens
Vice President for Academic Affairs and Provost (07/01/20 – present)	Dr. Andover Tarhule
Vice President for Academic Affairs and Provost (07/01/19 – 06/30/20)	Dr. Jan Murphy
Vice President for Student Affairs	Dr. Levester Johnson
Vice President for University Advancement	Mr. Pat Vickerman
Comptroller	Mr. Doug Schnittker
Legal Counsel	Ms. Lisa Huson
Director – Internal Audit	Mr. Robert Blemler

Officers of the Board of Trustees

Chair of the Board	Ms. Julie Annette Jones
Secretary of the Board	Dr. Mary Ann Louderback

Members of the Board of Trustees

Member	Ms. Kathryn Bohn
Member	Mr. Robert Dobski
Member	Mr. Rocky Donahue
Member	Ms. Julie Annette Jones
Member	Dr. Mary Ann Louderback
Member	Mr. Robert Navarro
Member (12/14/20 – present)	Vacant
Member (07/01/19 – 12/14/20)	Ms. Sharon Rossmark
Student Member (07/01/20 – present)	Ms. Jada Turner
Student Member (07/01/19 – 06/30/20)	Ms. Sarah Aguilar

Office Location

The University's primary administrative offices are located at:

Hovey Hall
Campus Box 1100
Normal, Illinois 61790-1100

**State of Illinois
Illinois State University**

**Financial Audit
For the Year Ended June 30, 2020**

Report Required Under *Government Auditing Standards*

Summary

The audit of the financial statements of the Illinois State University (University) was performed by RSM US LLP in accordance with *Government Auditing Standards*. This report is an integral part of that audit.

Based on their audit, the auditors expressed unmodified opinions on the University's basic financial statements, issued under a separate cover.

Summary of Findings

The auditors identified three matters involving the University's internal control over financial reporting that they considered to be material weaknesses and a significant deficiency. Further, the auditors identified one noncompliance matter.

<u>Item No.</u>	<u>Page</u>	<u>Last/First Reported</u>	<u>Description</u>	<u>Finding Type</u>
CURRENT FINDINGS				
2020-001	6	New	Inadequate Internal Controls over Census Data	Material Weakness and Noncompliance
2020-002	11	New	Lack of Adequate Controls over the Review of Internal Controls over Service Providers	Material Weakness
2020-003	13	2019/2018	Information Security Weaknesses	Significant Deficiency

**State of Illinois
Illinois State University**

**Financial Audit
For the Year Ended June 30, 2020**

Report Required Under *Government Auditing Standards*

Exit Conference

The findings and recommendations appearing in this report were discussed with University personnel at an exit conference on May 26, 2021. Attending were:

Illinois State University:

Dan Stephens	Vice President for Finance and Planning
Doug Schnittker	Comptroller
Erika Jones	Assistant Comptroller
Emily Duffield	Chief Accountant
Dan Taube	Interim Chief Information Security Officer
Charles Edamala	Associate Vice President and Chief Information Officer
Rob Blemler	Chief Internal Auditor

Office of the Auditor General:

Daniel J. Nugent, CPA	Technical Specialist
Reddy Bommareddi, CPA, CISA	Senior Audit Manager

RSM US LLP:

Joseph Evans, CPA	Partner
Dan Sethness, CPA	Senior Manager
Erik Ginter, CPA	Manager
Dan Harker	Manager

The response to the recommendations were provided by Ms. Erika Jones, Assistant Comptroller, in a correspondence dated May 27, 2021.



RSM US LLP

**Independent Auditor's Report on Internal Control Over Financial Reporting
and on Compliance and Other Matters Based on an Audit of Financial Statements
Performed in Accordance with *Government Auditing Standards***

Honorable Frank J. Mautino
Auditor General
State of Illinois

and

Board of Trustees
Illinois State University

Report on the Financial Statements

As Special Assistant Auditors for the Auditor General, we have audited, in accordance with the auditing standards generally accepted in the United States of America and the standards applicable to financial audits contained in *Government Auditing Standards* issued by the Comptroller General of the United States, the financial statements of the business-type activities and the aggregate discretely presented component units of the Illinois State University (University), collectively a component unit of the State of Illinois, as of and for the year ended June 30, 2020, and the related notes to the financial statements, which collectively comprise the University's basic financial statements, and we have issued our report thereon dated May 27 2021. Our report includes a reference to other auditors who audited the financial statements of the aggregate discretely presented component units, as described in our report on the University's financial statements. This report does not include the results of the other auditors' testing of internal control over financial reporting (internal control) or compliance and other matters of the Illinois State University Foundation and INTO Illinois State University, LLC, component units of the University, associated with these component units that are reported on separately by those auditors.

Compliance and Other Matters

As part of obtaining reasonable assurance about whether the University's financial statements are free from material misstatement, we performed tests of its compliance with certain provisions of laws, regulations, contracts, and grant agreements, noncompliance with which could have a direct and material effect on the financial statements. However, providing an opinion on compliance with those provisions was not an objective of our audit and, accordingly, we do not express such an opinion. The results of our tests disclosed an instance of noncompliance or other matters that is requested to be reported under *Government Auditing Standards* and which is described in the accompanying Schedule of Findings as item 2020-001.

Internal Control Over Financial Reporting

In planning and performing our audit of the financial statements, we considered the University's internal control over financial reporting (internal control) to determine the audit procedures that are appropriate in the circumstances for the purpose of expressing our opinions on the financial statements, but not for the purpose of expressing an opinion on the effectiveness of the University's internal control. Accordingly, we do not express an opinion on the effectiveness of the University's internal control.

Our consideration of internal control was for the limited purpose described in the preceding paragraph and was not designed to identify all deficiencies in internal control that might be material weaknesses or significant deficiencies and, therefore, material weaknesses or significant deficiencies may exist that have not been identified. However, as described in the accompanying Schedule of Findings, we did identify certain deficiencies in internal control that we consider to be material weaknesses and a significant deficiency.

A *deficiency in internal control* exists when the design or operation of a control does not allow management or employees, in the normal course of performing their assigned functions, to prevent, or detect and correct, misstatements on a timely basis. A *material weakness* is a deficiency, or a combination of deficiencies, in internal control, such that there is a reasonable possibility that a material misstatement of the entity's financial statements will not be prevented, or detected and corrected, on a timely basis. We consider the deficiencies described in the accompanying Schedule of Findings as items 2020-001 and 2020-002 to be material weaknesses.

A *significant deficiency* is a deficiency, or a combination of deficiencies, in internal control that is less severe than a material weakness, yet important enough to merit attention by those charged with governance. We consider the deficiencies described in the accompanying Schedule of Findings as item 2020-003 to be a significant deficiency.

University's Responses to the Findings

The University's responses to the findings identified in our audit are described in the accompanying Schedule of Findings. The University's responses were not subjected to the auditing procedures applied in the audit of the financial statements and, accordingly, we express no opinion on the responses.

Purpose of this Report

The purpose of this report is solely to describe the scope of our testing of internal control and compliance and the results of that testing, and not to provide an opinion on the effectiveness of the entity's internal control or on compliance. This report is an integral part of an audit performed in accordance with *Government Auditing Standards* in considering the entity's internal control and compliance. Accordingly, this communication is not suitable for any other purpose.

SIGNED ORIGINAL ON FILE

Schaumburg, Illinois
May 27, 2021

**State of Illinois
Illinois State University**

**Schedule of Findings
For the Year Ended June 30, 2020**

Current Findings – Government Auditing Standards

Finding 2020-001 Inadequate Internal Controls over Census Data

The Illinois State University (University) did not have adequate internal control over reporting its census data and did not have a reconciliation process 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 this 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.

We noted the University's employees are members of both 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, we noted these plans have characteristics of different types of pension and OPEB plans, including single employer plans and cost-sharing multiple-employer plans.

During testing, we noted the following:

- The University had not performed an initial complete reconciliation of its census data recorded by SURS and CMS to its internal records to establish a base year of complete and accurate census data.
- After establishing a base year, the University had not developed a process to annually obtain from SURS and CMS the incremental changes recorded by SURS and CMS in their census data records and reconcile these changes back to the University's internal supporting records.

Upon due consideration and based upon the significance of these issues alone, we concluded a material weakness exists within the University's internal controls related to ensuring both SURS and CMS can provide their respective actuaries with complete and accurate census data related to the University. Even given these two exceptions, we performed detail testing and certain data analysis tests and noted the following additional exceptions:

- 1) We performed an analysis of transactions reported by the University to SURS during the census data accumulation period throughout Fiscal Year 2018, noting the following problems:
 - Four of 505 (1%) employees reported as hired had actually been hired in other fiscal years. SURS determined the total potential impact to each employee's total service credit was it could be off by one-half to 4.25 years.

Schedule of Findings (Continued)
For the Year Ended June 30, 2020

Current Findings – Government Auditing Standards

Finding 2020-001 Inadequate Internal Controls over Census Data (Continued)

- Two of 33 (6%) employees with a departure on a leave of absence had the start date of the leave of absence untimely reported to SURS by the University. SURS determined the total potential impact to each of these employee's total service credit was it could be off by 1 to 1.75 years.
 - Five of 40 (13%) employees with a return from a leave of absence had the end date of the leave of absence untimely reported to SURS by the University. SURS determined the total potential impact to each of these employee's total service credit was it could be off by one-half to three-quarters of a year.
- 2) As of the end of the census data accumulation year on June 30, 2018, we identified two employees where each employee's associated termination or rehire date(s) had been untimely reported to SURS. While these employees were all associated with the University at June 30, 2018, some or all of these untimely reports may have occurred at other public universities and community colleges across the State. SURS determined these errors resulted in the employees being misclassified between the active, retired, and inactive member categories within SURS. The total potential impact to each former employee's total service credit was it could be off between 0.0 and 1.75 years.

For employers where their employees participate in plans with multiple-employer and cost-sharing features, the American Institute of Certified Public Accountants' *Audit and Accounting Guide: State and Local Governments* (AAG-SLG) (§ 13.177 for pensions and § 14.184 for OPEB) notes the determination of net pension/OPEB liability, pension/OPEB expense, and the associated deferred inflows and deferred outflows of resources depends on employer-provided census data reported to the plan being complete and accurate along with the accumulation and maintenance of this data by the plan being complete and accurate. To help mitigate against the risk of a plan's actuary using incomplete or inaccurate census data within similar agent multiple-employer plans, the AAG-SLG (§ 13.181 (A-27) for pensions and § 14.141 for OPEB) recommends an employer annually reconcile its active members' census data to a report from the plan of census data submitted to the plan's actuary, by comparing the current year's census data file to both the prior year's census data file and its underlying records for changes occurring during the current year.

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 a person who works for the University in a secretarial, mechanical, labor, clerical, educational, administrative, or other staff position which is either (a) permanent and continuous or (b) for a period of four months or an academic term, whichever is less, who is:

- 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;

**State of Illinois
Illinois State University**

**Schedule of Findings (Continued)
For the Year Ended June 30, 2020**

Current Findings – Government Auditing Standards

Finding 2020-001 Inadequate Internal Controls over Census Data (Continued)

- 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.

Further, for CMS' OPEB plan, we 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)).

In addition, the Illinois Pension 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 remit employer contributions to SURS reflecting the accruing normal costs of an employee paid from federal or trust funds. Additionally, the Act (5 ILCS 375/10) requires active employees to make contributions as set by CMS and the Act (5 ILCS 375/11) requires employer contributions by the University for all employees not totally compensated from its Income Fund, local auxiliary funds, and the Agricultural Premium Fund.

Finally, the Fiscal Control and Internal Auditing Act (30 ILCS 10/3001) requires the University 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 and statistical reports.

University officials indicated they routinely review and reconcile events in the SURS system based upon the data that is available but that a full reconciliation of the census data with SURS and CMS had not previously been completed because they were unaware the University needed to fully reconcile every census data element to SURS' and CMS' records. Additionally, with respect to the first data element, while the University has an established set of procedures sufficient to transmit census data to SURS, it appears inconsistent data arose between the University's HR system and SURS' system due to certain limited and unique circumstances, such as retroactive SURS eligibility, suffix correction, and transfer of benefits from another State school.

**State of Illinois
Illinois State University**

**Schedule of Findings (Continued)
For the Year Ended June 30, 2020**

Current Findings – Government Auditing Standards

Finding 2020-001 Inadequate Internal Controls over Census Data (Continued)

Recommendation

Failure to ensure complete and accurate census data was reported to SURS and CMS could have resulted in a material misstatement of the University's financial statements and reduced the overall accuracy of pension/OPEB-related liabilities, deferred inflows and outflows of resources, and expense recorded by the State, the State's agencies, and other public universities and community colleges across the State. In addition, failure to reconcile active members' census data reported to and held by SURS and CMS to the University's internal records could result in each plan's actuary relying on incomplete or inaccurate census data in the calculation of the University's pension and OPEB balances, which could result in a material misstatement of these amounts. (Finding Code No. 2020-001)

We recommend the University implement controls to ensure census data events are timely and accurately reported to SURS and CMS.

Further, we recommend the University work with SURS and CMS to develop an annual reconciliation process of its active members' census data from its underlying records to a report from each plan of census data submitted to the plan's actuary. After completing an initial full reconciliation, the University may limit the annual reconciliations 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.

Additionally, we recommend the University work with SURS and CMS to identify and address any unremitted or erroneously remitted employee and, if applicable, employer contributions related to these events.

Finally, due to the interrelatedness of SURS, the mobility of employees to change their employers within SURS, and a specific noncompliance matter regarding whether a person is eligible to participate in SURS identified during testing at Governors State University (please see Governors State University's Fiscal Year 2020 financial audit report for more information), we recommend the University work with both SURS and Governors State University to identify employees initially hired by Governors State University with a visa defined under subparagraphs (F), (J), (M), or (Q) of Section 1101(a)(15) of Title 8 of the United States Code who had not met the Internal Revenue Service's substantial presence test and started employment on and after July 1, 1991.

University Response

The University will continue to process SURS events based upon the information available at the time the employee begins employment with the University. In addition, as unique situations arise that require modifications to this data within the SURS system, the University will work with SURS to ensure that information is properly presented based on required compliance system parameters.

**State of Illinois
Illinois State University**

**Schedule of Findings (Continued)
For the Year Ended June 30, 2020**

Current Findings – *Government Auditing Standards*

Finding 2020-001 *Inadequate Internal Controls over Census Data (Continued)*

As a result of the new audit compliance procedures being required once GASB 75 was effective in fiscal year 2018, the University has correspondingly identified some unknown gaps in existing procedures that led to the late reporting of leave of absences. Upon notice, appropriate steps were taken to address this gap.

The University will continue to independently review the visa status of new employees and determine their state tax residency status for tax purposes, even those that are transferring from another State of Illinois University.

Finally, from this point forward, the University will be performing additional census testing in coordination with the SURS' Special Assistant Auditors to help identify and reconcile identified data errors and inconsistencies. In addition, the University will dedicate extra staff resources to focus greater attention on working with SURS, CMS, and other State schools to establish jointly agreed upon procedures leading to a more comprehensive reconciliation process for the census data. We welcome this partnership approach with SURS, CMS and the Office of the Auditor General.

**State of Illinois
Illinois State University**

**Schedule of Findings (Continued)
For the Year Ended June 30, 2020**

Current Findings – Government Auditing Standards

Finding 2020-002 Lack of Adequate Controls over the Review of Internal Controls over Service Providers

The Illinois State University (University) did not obtain or conduct timely independent internal controls reviews over its service providers.

We requested the University provide a listing of service providers utilized in order to determine if the University had reviewed the internal controls over their service providers. However, the University was unable to provide a listing of service providers utilized during the examination period.

Due to these conditions, we were unable to conclude the University's population records were complete and accurate under the Professional Standards promulgated by the American Institute of Certified Public Accountants (AU-C § 500, AU-C § 530, and AT-C § 205.35).

Even though the University did not provide a listing of service providers, we determined the University utilized service providers for hosting:

- a system containing significant amounts of data and student records protected by the federal Family Education Rights and Privacy Act (FERPA);
- a system which maintains prospective and new student information; and,
- the University's payroll application with Human Resources (HR) functionality.

The University did not have a program to obtain and review System and Organization Control (SOC) reports. In addition, the University did not track compliance with service levels agreed to with the service providers.

The University is responsible for the design, implementation, and maintenance of internal controls related to information systems and operations to assure its critical and confidential data are adequately safeguarded. This responsibility is not limited due to the processes being outsourced.

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 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 and to maintain accountability over the State's resources.

In addition, 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 through SOC reports or independent reviews.

University officials indicated they were unaware of the need to centrally track all service providers and obtain and review SOC reports and compliance with service level agreements.

**State of Illinois
Illinois State University**

**Schedule of Findings (Continued)
For the Year Ended June 30, 2020**

Current Findings – Government Auditing Standards

**Finding 2020-002 Lack of Adequate Controls over the Review of Internal Controls over
Service Providers (Continued)**

Without having obtained and reviewed a SOC report or another form of independent internal controls review, the University does not have assurance the service providers' internal controls are adequate to ensure its critical and confidential data are secure and available. In addition, failure to ensure compliance with service level agreements may lend itself to inadequate services by the service provider. (Finding Code No. 2020-002)

Recommendation

We recommend the University identify all service providers and determine and document if a review of internal controls is required. If required, the University should:

- obtain SOC reports or perform independent reviews of internal controls associated with outsourced systems at least annually;
- monitor and document the operation of the Complementary User Entity Controls (CUECs) relevant to the University's operations; and,
- review service level agreements with service providers to ensure applicable requirements are met.

In addition, if a SOC report indicates one or more subservice providers exist, the University should:

- either obtain and review a SOC report for each subservice organization or perform alternative procedures to satisfy the usage of each subservice organization would not impact the University's internal control environment; and,
- document its review of the SOC reports and review all significant issues with each subservice organization to ascertain if a corrective action plan exists and when it will be implemented, any impacts to the University, and any compensating controls.

University Response

The University recognizes the importance of vendor risk management. While it has careful control over procurement and data usage regarding service providers, processes to maintain the assurance over information and information systems are not in place. The University will work to develop, release, and enforce vendor management procedures and standards that will address these findings.

**State of Illinois
Illinois State University**

**Schedule of Findings (Continued)
For the Year Ended June 30, 2020**

Current Findings – Government Auditing Standards

Finding 2020-003 Information Security Weaknesses

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 the University's needs.

During testing, we identified the following security weaknesses:

- The University's Information Technology (IT) policies and procedures were not reviewed and updated during the examination period to reflect the University's current environment or address future changes in processes and new systems.
- The University did not conduct a user access review for all of its applications, including a review of administrative access.
- The University did not conduct segregation of duties reviews between development and production environments for systems where University personnel have development responsibilities.
- The University's Center for Teaching, Learning, and Technology (CTLT), an academic unit, granted local administrative privileges by default to all users on their endpoint devices.
- The University was unable to provide access approval evidence for 2 of 40 (5%) access requests tested.
- Five of 37 (14%) terminated employees' accounts tested were not timely removed. The five noted accounts had access removed between 90 and 365 days after the associated employee separated from the University.
- For a financial application, we noted users' accesses were not timely removed and were able to retain access up to one year until the user's network account was removed.
- The University did not timely patch its system endpoints and servers. We noted 1,262 of 9,069 (14%) desktop endpoints and 216 of 706 (31%) servers were not patched.

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 University funds, property, and resources are safeguarded against waste, loss, unauthorized use, and misappropriation.

In addition, 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 section, sanctions the appropriateness of access rights, timely termination, and periodic review of access rights to ensure appropriateness. Additionally, Special Publication 800-53's Configuration Management section, enforces logical restrictions with changes to systems.

**State of Illinois
Illinois State University**

**Schedule of Findings (Continued)
For the Year Ended June 30, 2020**

Current Findings – Government Auditing Standards

Finding 2020-003 Information Security Weaknesses (Continued)

University officials indicated:

- 1) the policies were drafted and presented to the University's executive management team; however, these policies were not formally adopted due to the COVID-19 pandemic;
- 2) the user access and segregation of duties reviews were not completed due to other competing priorities;
- 3) they were unaware CTLT granted local administrative privileges by default to all users on their endpoint devices;
- 4) access approval documentation was not retained due to employee oversight;
- 5) terminated employees' accounts were not timely removed due to employee oversight;
- 6) they were unaware access to the noted financial application could potentially remain available to terminated users for up to a year; and,
- 7) underperformance of patch management was due to the decentralized nature of support operations across the University without a single entity providing direction and oversight.

Failure to maintain current policies and procedures could result in the University's security requirements not being met. Additionally, failure to maintain documentation on access approvals and review of all access rights could result in unauthorized access and modification to the University's systems. Also, failure to timely patch information systems could result in a compromise and expose confidential, sensitive, or personal information to unauthorized parties. (Finding Code No. 2020-003, 2019-001, 2018-002)

Recommendation

We recommend the University implement adequate security, including:

- finalizing the policies and procedures to (1) reflect the University's current environment and (2) address future changes in processes and new systems;
- conducting formal user access reviews, which includes (1) all privileged access to the system, (2) critical business functions, and (3) business or IT segregation of duties conflicts;
- restricting privileged access to the minimum number of users necessary;
- ensuring all access requests are approved and documentation is retained;
- ensuring access to all applications is terminated in a timely manner; and,
- ensuring all devices are timely patched with vendor updates.

University Response

The University recognizes that this finding is a combination of weaknesses from the FY19 audit period as well as new ones from the FY20 audit period.

Regarding the FY19 items specifically, the University has made considerable progress on corrective actions. However, due to the direct impact of the COVID-19 pandemic, the University experienced resource constraints and technical limitations that prevent it from fully addressing all issues.

**State of Illinois
Illinois State University**

**Schedule of Findings (Continued)
For the Year Ended June 30, 2020**

Current Findings – Government Auditing Standards

Finding 2020-003 Information Security Weaknesses (Continued)

The University will pursue the following corrective actions to address these items:

- To address University policies and procedures:
 - Continue working through institutional process to release new and updated documents.
 - Develop and release departmental procedures that align with the in-progress University policies for rapid adoption.
- To address access management:
 - Develop, release, and enforce an access review procedure and standard to be implemented with system administrators and owners.
 - Develop and enhance system integrations to automatically remove access as part of data entry for terminations.
 - Develop, release, and enforce a user access standard for University-owned endpoint devices that prohibits defaulting to local administrator.
- To address system management:
 - Develop, release, and enforce a patch management standard for University-owned endpoint and server devices.

In support of these corrective actions, and ultimately the enhancement of information security at the University, the Information Security Program will continue to align with the NIST Cybersecurity Framework, conducting gap analysis and implementation efforts for the covered functions.