DEPARTMENT OF INNOVATION AND TECHNOLOGY
INFORMATION TECHNOLOGY HOSTING SERVICES

System and Organization Control Report and Report Required Under *Government Auditing Standards* For the Year Ended June 30, 2021

Release Date: August 12, 2021

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

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

*This is the first examination of the "Description of the State of Illinois, Information Technology Hosting Services".

INTRODUCTION

This digest covers our System and Organization Control Report (SOC 2) and Report Required *Under Government Auditing Standards* of the Department of Innovation and Technology (Department), Information Technology Hosting Services for the period from July 1, 2020 through June 30, 2021.

The System and Organization Control Report contained a modified opinion due to the weaknesses associated with the Department's operating effectiveness of controls. In addition, the Report Required Under *Government Auditing Standards* (GAS) contains one finding.

SYNOPSIS

• (**21-01**) The Department did not ensure its controls over the Information Technology Hosting Services operated effectively.

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

CONTROLS DID NOT OPERATE EFFECTIVELY

Controls did not operate effectively

The Department of Innovation and Technology (Department) did not ensure its controls over the Information Technology Hosting Services operated effectively. The controls related to the control objectives are stated in the "Description of the State of Illinois, Information Technology Hosting Services" (description), provided by the Department.

Populations were not provided to conduct tests of controls

As part of our testing to determine if the controls were operating effectively, we requested the Department to provide a population of modifications to employees' and contractors' access to the Department's resources. However, the Department was unable to provide a population. As a result of the Department's inability to provide the population, we were unable to conduct testing to determine if the controls related to logical access to applications, data, and the environment were restricted to authorized and appropriate users.

Additionally, we requested the Department provide a population of modified security software IDs during the examination period. However, the Department was unable to provide a population. As a result of the Department's inability to provide the population, we were unable to conduct testing to determine if the controls related to logical access to applications, data, and the environment were restricted to authorized and appropriate users.

Furthermore, during our testing of the controls related to the control objectives stated in the description of system, we noted specific controls which did not operate effectively. Specifically, we noted:

Human resources weaknesses

Human Resources
- Employee evaluations were not completed within the defined timeline.
- Employees and contractors did not complete or completed late the Ethics Training Program and the Security Awareness Training.

Policies and procedures weaknesses

Policies and Procedures
- The Department did not have a policy or procedure documenting the frequency in which policies and procedures published on its website were to be reviewed.

Subservice providers weaknesses

Subservice Providers
- Subservice providers' contracts did not contain the requirement for the subservice provider to contact the Department in the event of a security incident or breach.

	• System and Organization Control (SOC) reports were not received from all subservice providers.
Risk weaknesses	<u>Risk</u> • Agencies' risk assessments were not always conducted. • Vulnerability scans were not communicated to all Group Chief Information Officers and Agency Chief Information Officers. • Upon notification of the closure of medium and high priority threats, Executive Summaries were not sent to the Chief Information Security Officer or the Deputy Chief Information Security Officer. • An agency was not notified of a medium threat in order to determine the impact to users.
Logical access provisioning and de-provisioning weaknesses	<u>Logical Access Provisioning and De-Provisioning</u> • The Department did not have a policy documenting the required timeframe for revocation of logical access upon termination. • The Department did not conduct the Security Software Annual Reconciliation. • New security software accounts were not approved by the Agency Technology Service Requestor. • New security software accounts did not have an approved Remedy ticket or Mainframe Access Request Form. • The Department could not provide documentation demonstrating separated individuals' access rights were terminated. • Terminated employees did not have a Remedy Service Request completed.
Physical access provisioning and de-provisioning weaknesses	<u>Physical Access Provisioning and De-Provisioning</u> • The Department was unable to provide documentation demonstrating the timely termination of individuals' access to the Department's resources. • New employee and contractor access requests were not properly completed. • Individuals were provided inappropriate access to Department facilities.
Change management weaknesses	<u>Change Management</u> • The Remedy on Demand User Guide contradicted the Change Management Guide requirements for required approvals. • Changes did not always have test plans, backout plans, or implementation plans. • Changes were not approved by the Change Advisory Committee, Enterprise Change Manager, or Group Manager. • Changes classified as 'No Impact' were not reviewed monthly.

- Emergency changes did not always have a Post Implementation Review conducted.

Network weaknesses

Network
- Systems were not up-to-date with the latest anti-virus software.
- Operating system patches were not tested or did not have documentation of testing prior to being pushed to the general populations.
- A Network Administrator did not require administrative rights to the environment.
- Device configurations were not backed up for the period of April 15 to April 23, 2021.

As a result of the above noted exceptions, the controls were not operating effectively to provide reasonable assurance the control objectives stated in the description were achieved resulted in a modified opinion on the Department's System and Organization Control Report. (Finding 1, pages 7-9)

We recommended the Department ensure its controls operate effectively over the services provided to the user entities.

Department agreed with Service Auditor

Department officials accepted the recommendation.

DEPARTMENT SECRETARY

During Examination Period:
Jennifer Ricker, Acting (9/5/20 – Present)
Ron Guerrier (7/1/20 – 9/4/20)

SERVICE AUDITOR'S OPINION

The System and Organization Control Report contained a modified opinion. Specifically, the Service Auditors determined, except for the matters described in the System and Organization Control Report, in all material respects, based on the criteria described in the State of Illinois, Department of Innovation and Technology's assertion:

a. the description presents the State of Illinois, Information Technology Hosting Services that was designed and implemented throughout the period July 1, 2020 to June 30, 2021 in accordance with the description criteria.

b. the controls stated in the description were suitably designed throughout the period July 1, 2020 to June 30, 2021 to provide reasonable assurance that the Department's service commitments and system requirements would be achieved based on the applicable trust services criteria, if its controls

iv

operated effectively throughout that period and if the subservice organizations and user entities applied the complementary controls assumed in the design of the Department's controls throughout that period.

   c. The controls stated in the description operated effectively throughout the period July 1, 2020 to June 30, 2021, to provide reasonable assurance that the Department's service commitments and system requirements were achieved based on the applicable trust services criteria if complementary subservice organization controls and complementary user entity controls assumed in the design of the Department's controls operated effectively throughout that period.

This System and Organization Control Examination was conducted by the Office of the Auditor General's staff.

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:MKL