DEPARTMENT OF INNOVATION & TECHNOLOGY

Report Required Under
Government Auditing Standards

FOR THE PERIOD
JULY 1, 2017 – JUNE 30, 2018

TABLE OF CONTENTS

DEPARTMENT OF INNOVATION & TECHNOLOGY
Department Officials

Secretary, Acting (9/18/17-Current)	Kirk Lonbom
Secretary Designate (7/1/17-9/17/17)	Hardik Bhatt
Chief Internal Auditor	Doug Tinch
Affirmative Action/Equal Employment Opportunity Officer	Vickie Simpson
Chief Administrative Officer (5/1/18-Current)	Clark Kaericher
Chief Administrative Officer (7/1/17-4/30/18)	Vacant
Chief Service Officer	Vacant
Chief of Staff	Tyler Clark
ERP Program Director	Kevin O'Toole
Chief Strategy Officer (5/16/18-Current)	Shannon Rahming
Chief Strategy Officer (7/1/17-5/15/18)	Vacant
Chief Technology Officer (4/16/18-Current)	John King
Chief Technology Officer (1/16/18-4/15/18)	Vacant
Chief Technology Officer (7/1/17-1/15/18)	Michael Wons
Chief Information Security Officer (4/16/18-Current)	Chris Hill
Chief Information Security Officer, Acting (9/18/17-4/15/18)	Chris Hill
Chief Information Security Officer (7/1/17-9/17/17)	Kirk Lonbom
Cluster Chief Information Officers:	
Family, Children, Elderly & Veterans	Brad Long
Government & Public Employees	Monica Carranza
Business & Workforce	Sunil Thomas
Natural & Cultural Resources (4/1/18-Current)	Vacant
Natural & Cultural Resources (10/1/17-3/31/18)	Mark Kinkade
Natural & Cultural Resources (9/16/17-9/30/17)	Vacant
Natural & Cultural Resources (7/1/17-9/15/17)	Philip Buche

Cluster Chief Information Officers (continued):

Public Safety (9/16/17-Current)	Steve Buche
Public Safety (7/1/17-9/15/17)	Herbert Dodson
Students (9/16/17-Current)	Vacant
Students (7/1/17-9/15/17)	George Wang
Transportation	Vacant

The Department's administrative office is located at:
120 West Jefferson Street
Springfield, Illinois 62702

DEPARTMENT OF INNOVATION & TECHNOLOGY
GOVERNMENT AUDITING STANDARDS REPORT

Government Auditing Report Summary

The examination of the "Description of the IT General Controls and Application Controls for the Department of Innovation & Technology's Information Technology Shared Services system" (Service Organization Control Report) was performed by the Office of the Auditor General in accordance with *Government Auditing Standards.* Based on their examination, the Service Auditors expressed an adverse opinion on the Department's Description of the information technology general controls and application controls for the Department of Innovation & Technology's Information Technology Shared Services System. The Service Organization Control Report was issued under separate cover dated August 8, 2018.

Summary of Findings

The Service Auditors identified certain deficiencies in internal control over the "Description of the IT General Controls and Application Controls for the Department of Innovation & Technology's Information Technology Shared Services system" that they consider to be material weaknesses, which are described in the accompanying Schedule of Finding on pages 7-13 of this report as Finding 2018-001, *Inaccurate Description of System*, Finding 2018-002, *Controls Were Not Suitably Designed*, and Finding 2018-003, *Controls Did Not Operate Effectively.*

Exit Conference

The findings and recommendations appearing in this report were discussed with the Department at an exit conference on August 3, 2018. Attending were:

Kirk Lonbom, Acting Secretary
Tyler Clark, Chief of Staff
Doug Tinch, Chief Internal Auditor
Shannon Rahming, Chief Strategy Officer
Kevin O'Toole, ERP Program Director
Barb Piwowarski, ERP Program Manager
Sree Nair, Project Manager, Security

Kathy Lovejoy, Senior Manager, Office of the Auditor General
Brian Metzger, Supervisor, Office of the Auditor General

The responses to the recommendations were provided by Sree Nair, Audit Liaison, via email dated August 6, 2018.

SPRINGFIELD OFFICE:

ILES PARK PLAZA

740 EAST ASH • 62703-3154

PHONE: 217/782-6046

CHICAGO OFFICE:

MICHAEL A. BILANDIC BLDG. • SUITE S-900

160 NORTH LASALLE • 60601-3103

PHONE: 312/814-4000

OFFICE OF THE AUDITOR GENERAL

FRANK J. MAUTINO

INDEPENDENT SERVICE AUDITOR'S REPORT ON INTERNAL CONTROL OVER REPORTING AND ON COMPLIANCE AND OTHER MATTERS BASED ON AN EXAMINATION OF A SERVICE ORGANIZATION PERFORMED IN ACCORDANCE WITH *GOVERNMENT AUDITING STANDARDS*

Honorable Frank J. Mautino
Auditor General
State of Illinois

We have examined, in accordance with the attestation standards established by the American Institute of Certified Public Accountants and the standards applicable to attestation engagements contained in *Government Auditing Standards* issued by the Comptroller General of the United States, the State of Illinois, Department of Innovation & Technology's "Description of the IT General Controls and Application Controls for the Department of Innovation & Technology's Information Technology Shared Services system" (description) for the information technology general controls and application controls throughout the period July 1, 2017, through June 30, 2018, and have issued our report thereon under separate cover dated August 8, 2018.

Internal Control over Reporting

Management of the State of Illinois, Department of Innovation & Technology is responsible for establishing and maintaining effective internal control over (1) fairly presenting the State of Illinois, Department of Innovation & Technology's description for the information technology general controls and application controls throughout the period July 1, 2017, through June 30, 2018, and (2) establishing and maintaining effective internal control over the suitable design and operating effectiveness of the controls related to the control objectives within the State of Illinois, Department of Innovation & Technology's description for the information technology general controls and application controls throughout the period July 1, 2017, through June 30, 2018 (internal control over reporting). In planning and performing our examination, we considered the State of Illinois, Department of Innovation & Technology's internal control over reporting to determine the examination procedures that are appropriate in the circumstances for the purpose of expressing our opinion on the State of Illinois, Department of Innovation & Technology's description for the information technology general controls and application controls throughout the period July 1, 2017, through June 30, 2018, but not for the purpose of expressing an opinion on the effectiveness of the State of Illinois, Department of Innovation & Technology's internal

control over reporting. Accordingly, we do not express an opinion on the effectiveness of the State of Illinois, Department of Innovation & Technology's internal control over reporting.

A *deficiency in internal control over reporting* 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 in internal control over reporting* is a deficiency, or a combination of deficiencies, in internal control such that there is a reasonable possibility that a material misstatement of the Department's description will not be prevented, or detected and corrected on a timely basis. A *significant deficiency in internal control over reporting* 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.

Our consideration of internal control over reporting was for the limited purpose described in the first paragraph of this section and was not designed to identify all deficiencies in internal control over reporting that might be material weaknesses or significant deficiencies and, therefore, material weaknesses or significant deficiencies may exist that were not identified. We did identify certain deficiencies in internal control, described in the accompanying schedule of findings as items 2018-001 through 2018-003, that we consider to be material weaknesses.

Compliance and Other Matters

As part of obtaining reasonable assurance about whether the State of Illinois, Department of Innovation & Technology's description for the information technology general controls and application controls throughout the period July 1, 2017, through June 30, 2018, is fairly presented and the controls related to the control objectives in the State of Illinois, Department of Innovation & Technology's description for the information technology general controls and application controls throughout the period July 1, 2017, through June 30, 2018, were suitably designed and operating effectively, 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 State of Illinois, Department of Innovation & Technology's description for the information technology general controls and application controls throughout the period July 1, 2017, through June 30, 2018. However, providing an opinion on compliance with those provisions was not an objective of our examination and, accordingly, we do not express such an opinion. The results of our tests disclosed no instances of noncompliance or other matters that are required to be reported under *Government Auditing Standards*.

State of Illinois, Department of Innovation & Technology's Response to Findings

The State of Illinois, Department of Innovation & Technology's responses to the internal control findings identified in our examination are described in the accompanying schedule of findings. The State of Illinois, Department of Innovation & Technology's responses were not subjected to the procedures applied in the examination 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 over reporting and compliance and the results of that testing, and not to provide an opinion on the effectiveness of the State of Illinois, Department of Innovation & Technology's internal control over reporting or on compliance. This report is an integral part of an examination performed in accordance with *Government Auditing Standards* in considering the State of Illinois, Department of Innovation & Technology's internal control and compliance. Accordingly, this communication is not suitable for any other purpose.

SIGNED ORIGINAL ON FILE

William J. Sampias, CISA
Director, Information Systems Audits

SIGNED ORIGINAL ON FILE

Mary Kathryn Lovejoy, CPA, CISA
Senior Audit Manager

Springfield, Illinois
August 8, 2018

DEPARTMENT OF INNOVATION & TECHNOLOGY
CURRENT FINDINGS-*GOVERNMENT AUDITING STANDARDS*
For the Year Ended June 30, 2018

2018-001 **Finding** Inaccurate Description of System

The "Description of the IT General Controls and Application Controls for the Department of Innovation & Technology's Information Technology Shared Services system" (description of system), as provided by the Department of Innovation & Technology (Department), contained inaccuracies and omissions.

The Department provides State agencies with an information technology general controls and application controls for their use. As such, the Department, as a service provider, provides services which are likely relevant to user agencies' internal control over financial reporting. Therefore, the Department is required to develop an accurate and complete description of system documenting its internal controls over the services provided.

During our examination of the Department's description of system, we noted:

- it contained inaccurate statements. Specifically, we noted the description of system stated:
  - the IT Risk Assessment Policy was no longer utilized by the Department and was not located on the Department's website;
  - all job descriptions were not approved by the Department of Central Management Services' (DCMS) Division of Technical Services;
  - ethics training and the DCMS Policy Manual was not provided to newly hired vendor contractors;
  - developers did not obtain user acceptance approvals over changes to the Common Systems;
  - separation reports were not provided to the Security Software Administrator bi-monthly;
  - Remote Monitoring Facility reports were not run weekly;
  - data file transmissions did not always utilize standard processes;
  - errors that occurred on data file transmission were not always sent to the Production Control Team for resolution, recorded in the Shift Change Checklist, or generated a Remedy ticket;
  - the Enterprise Storage and Backup group was not notified of disc or hardware failures; and
  - preventive maintenance agreements for the water detection system had not been established.

- it omitted internal controls. Specifically, the description of system did not include:
  - complementary subservice organization controls for the subservice providers they utilized;
  - information regarding the configuration standards and installation requirements for midrange devices;
  - information on the secondary mainframe operating system;

- all interfaces and protocols available to user agencies to transmit data;
- the process for termination of physical access when an individual no longer required access; and
- the mass approval and load process for users transitioning to the ERP.

The Fiscal Control and Internal Auditing Act (30 ILCS 10/3001) requires the Department to establish and maintain a system, or systems, of internal fiscal and administrative controls to provide assurance that resources and 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.

Department management indicated the errors were due to oversight.

Failure to provide an accurate and complete description of system resulted in an adverse opinion on the Department's Service Organization Control Report. Additionally, without an accurate and complete description of system, the user agencies' internal control over financial reporting may have unidentified deficiencies and the user agencies' auditors are unable to rely on the internal controls related to the services provided by the Department. (Finding Code 2018-001)

Recommendation

We recommend the Department review the description of system to ensure it is complete, accurate, and contains all internal controls over the services provided to user agencies.

Department Response

The Department agrees with the finding. The Department will review the Description of Service to ensure the description is complete, accurate and contains all the internal controls over the services provided to user agencies.

DEPARTMENT OF INNOVATION & TECHNOLOGY
CURRENT FINDINGS-*GOVERNMENT AUDITING STANDARDS*
For the Year Ended June 30, 2018

2018-002 Finding Controls Were Not Suitably Designed

The controls related to the control objectives stated in the "Description of the IT General Controls and Application Controls for the Department of Innovation & Technology's Information Technology Shared Services system" (description of system), as provided by the Department of Innovation & Technology (Department), were not suitably designed to provide reasonable assurance the control objectives would be achieved.

As part of testing to determine if the controls were suitably designed, we requested the Department to provide populations related to:

- Major outage or infrastructure failures,
- eTime Administrators,
- Modifications to access rights, and
- Physical security incident reports.

However, the Department did not provide complete and accurate populations. Due to these conditions, we were unable to conclude the Department's population records were sufficiently precise and detailed under the Attestation Standards promulgated by the American Institute of Certified Public Accountants (AT-C §320.30) to test the suitable design of the controls. As such we could not perform detailed testing.

In addition, during our testing, we noted:

- IL ACT (ERP) Change Management Policy & Procedures did not document who was to approve requests;
- IL ACT (ERP) Change Management Policy & Procedures did not provide sufficient detail to determine that change requests were properly completed, validated, reviewed and approved;
- The Department did not maintain documentation of the annual review of security software IDs with powerful privileges;
- The Department did not maintain documentation of the reviews of Incident Reports by the Chief Information Security Officer;
- The Department did not maintain documentation of the weekly reviews of System Management Facility records; and
- The Department did not maintain documentation of assessments of newly discovered vulnerabilities.

As a result of the above noted exceptions, we were unable to determine if the controls were suitably designed.

The Fiscal Control and Internal Auditing Act (30 ILCS 10/3001) requires the Department to establish and maintain a system, or systems, of internal fiscal and administrative controls to provide assurance that resources and 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. Furthermore, the State Records Act (5 ILCS 160/8) requires the Department to make and reserve records containing adequate and proper documentation of the functions, policies, decisions, procedures, and actions of the Department in order to protect the legal and financial rights of the State.

Department management indicated the errors were due to oversight.

Failure to provide controls that were suitably designed resulted in an adverse opinion on the Department's Service Organization Control Report. Additionally, without controls that are suitably designed at the Department, the user agencies' auditors will be unable to rely on the operating effectiveness of the Department's controls over the user agencies' internal control over financial reporting. (Finding Code 2018-002)

Recommendation

We recommend the Department ensure the controls are suitably designed over the services provided to user agencies.

Department Response

The Department agrees with the finding. The Department will review and implement controls to ensure that they are suitably designed over the services provided to user agencies.

DEPARTMENT OF INNOVATION & TECHNOLOGY
CURRENT FINDINGS-*GOVERNMENT AUDITING STANDARDS*
For the Year Ended June 30, 2018

2018-003 Finding Controls Did Not Operate Effectively

The controls related to the control objectives stated in the "Description of the IT General Controls and Application Controls for the Department of Innovation & Technology's Information Technology Shared Services system" (description of system), provided by the Department of Innovation & Technology (Department), did not operate effectively.

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:

Policies and Procedures
The following policies and procedures did not provide guidance related to areas such as prioritization of requests, required approvals, testing and documentation requirements, and requirements for post implementation reviews.

- The Remedy Change Management Guide;
- The Application Lifecycle Management Manual;
- The EAA Project Development Web Methodology; and
- The IL ACTS (ERP) Change Management Policy & Procedures.

In addition, we found:

- the MORT Initiation Procedures did not address the after- hours processes;
- the Missing IT Equipment Procedures did not address the process in the event encryption was not installed; and
- the policies and procedures governing logical security did not address the requirements for requesting, obtaining and modifying access rights, periodic review of access rights, and revocation of access rights.

Human Resources
We found multiple instances where employees or contractors:

- had not completed security awareness training or cybersecurity training;
- did not have a probationary or annual evaluation completed or it was completed late; and
- had not completed the annual acknowledgement of compliance with security policies.

Access Provisioning and De-Provisioning
We found multiple instances where employees or contractors did not have authorization to obtain access rights. In other instances, the request forms were submitted late or not properly approved. In addition, access rights were not always removed timely and separation reports were not always reviewed.

Application Edits

- Multiple ERP transaction codes were still active even though they were no longer utilized by the Department.
- An edit check to prevent duplicate asset tag numbers had not been implemented.
- Nineteen states with income tax requirements were not included in the Central Payroll System (CPS) tax tables.
- 3 States' tax rates were incorrect in the CPS tax tables.

Change Management

We found instances where ERP change requests were not properly completed and approved. In addition, an infrastructure emergency change was not reviewed and discussed at the weekly Change Advisory Committee meeting and the Enterprise Change Manager did not review transparent changes monthly.

Device Configurations

The required security banner warning of prosecution for unauthorized access was not always displayed at initial sign-on. In addition 551 laptops and desktops were not up-to-date with the latest anti-virus product and 3,692 were not up-to-date with the latest anti-virus definitions.

Environmental Factors

We found instances where physical security daily activity reports could not be provided. In addition, the Department did not have a maintenance contract in place for the generator located at the Central Computing Facility and the maintenance contract for the Communication Building generator expired on January 31, 2018. Also, the Department did not maintain a maintenance contract for the Communication Building uninterruptable power supply.

As a result of the above noted exceptions, the controls were not operating effectively to provide reasonable assurance that the control objectives stated in the description were achieved

The Fiscal Control and Internal Auditing Act (30 ILCS 10/3001) requires the Department to establish and maintain a system, or systems, of internal fiscal and administrative controls to provide assurance that resources and 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.

Department management indicated the errors were due to oversight, staffing shortages and human error.

Failure to ensure controls operated effectively to provide reasonable assurance that the control objectives stated in the description were achieved resulted in an adverse opinion on the Department's Service Organization Control Report. Additionally, without effective operating controls, the user agencies' auditors will be unable to rely on the operating effectiveness of the controls impacting the user agencies' internal control over financial reporting. (Finding Code 2018-003)

Recommendation

We recommend the Department ensure its controls operate effectively over the services provided to user agencies.

Department Response

The Department agrees with the finding. The Department will review and monitor controls to ensure that they operate effectively over the services provided to user agencies.