New York State Office of the State Comptroller
Thomas P. DiNapoli

Division of State Government Accountability

Security Over Critical Information Systems

State Education Department

Executive Summary

Purpose

To determine whether the security controls over critical State Education Department (Department) information systems were sufficient to minimize the various risks associated with unauthorized access to these systems and their associated data. Our audit scope covers the period September 29, 2016 through March 30, 2017.

Background

The Department administers school aid, regulates school operations, maintains a performance accountability system, oversees the licensing of numerous professions, certifies teachers, and administers a host of other educational programs. Its responsibilities include oversight of more than 700 school districts with 3.2 million students, 7,000 libraries, 900 museums, and 52 professions encompassing more than 850,000 licensees. The Department operates 120 computer systems to help support its activities, including four deemed critical to Department operations that we focused our testing on. Each of the four systems supports crucial Department services to the general public and contains sensitive personal data, such as personally identifiable information and student records. The Department is responsible for safeguarding its data and for ensuring the confidentiality, integrity, and availability of its systems.

Key Findings

- While the Department has taken a number of steps to secure its critical information systems and associated data, there is a risk that unauthorized persons could access these systems. This is largely because the Department has not taken fundamental steps to secure its critical systems, such as completing a full data classification process and adopting adequate information security policies and procedures.
- The Department could also improve certain technical controls over its critical systems.

Key Recommendations

- Develop strategies to enhance security controls over critical systems.
- Implement the recommendations detailed during the audit to strengthen technical controls over critical systems.

Other Related Audits/Reports of Interest

Central New York Regional Transportation Authority: Compliance With Payment Card Industry Standards (2016-S-31)

Office of Information Technology Services: Security and Effectiveness of Department of Motor Vehicles' Licensing and Registration Systems (2013-S-58)

**State of New York
Office of the State Comptroller**

Division of State Government Accountability

July 19, 2017

Ms. MaryEllen Elia
Commissioner
State Education Department
State Education Building - Room 125
89 Washington Avenue
Albany, NY 12234

Dear Commissioner Elia:

The Office of the State Comptroller is committed to helping State agencies, public authorities, and local government agencies manage government resources efficiently and effectively. By doing so, it provides accountability for tax dollars spent to support government operations. The Comptroller oversees the fiscal affairs of State agencies, public authorities, and local government agencies, as well as their compliance with relevant statutes and their observance of good business practices. This fiscal oversight is accomplished, in part, through our audits, which identify opportunities for improving operations. Audits can also identify strategies for reducing costs and strengthening controls that are intended to safeguard assets.

Following is a report of our audit entitled *Security Over Critical Information Systems*. The audit was performed pursuant to the State Comptroller's authority as set forth in in Article V, Section 1 of the State Constitution and Article II, Section 8 of the State Finance Law.

This audit's results and recommendations are resources for you to use in effectively managing your operations and in meeting the expectations of taxpayers. If you have any questions about this report, please feel free to contact us.

Respectfully submitted,

*Office of the State Comptroller
Division of State Government Accountability*

Table of Contents

State Government Accountability Contact Information:
Audit Director: Brian Reilly
Phone: (518) 474-3271
Email: StateGovernmentAccountability@osc.state.ny.us
Address:
   Office of the State Comptroller
   Division of State Government Accountability
   110 State Street, 11th Floor
   Albany, NY 12236

This report is also available on our website at: www.osc.state.ny.us

Background

The State Education Department (Department) administers school aid, regulates school operations, maintains a performance accountability system, oversees the licensing of numerous professions, certifies teachers, and administers a host of other educational programs. These include special education services, cultural education programs such as the State Museum and the State Archives, higher and professional education programs, vocational rehabilitation, and adult career and continuing education services. The Department has eight main branches: Office of P-12 Education, Office of Higher Education, Office of Cultural Education, Office of Performance Improvement and Management Services, Chief Financial Officer, Office of Counsel, Office of Professions, and Office of Adult Career and Continuing Education Services. Its responsibilities include oversight of more than 700 school districts with 3.2 million students, 7,000 libraries, 900 museums, and 52 professions encompassing more than 850,000 licensees.

The Department operates many critical computer systems to help support its activities, a number of which routinely collect, process, and store sensitive personally identifiable information and student data. Without proper safeguards, computer systems are vulnerable to individuals and groups with malicious intentions, who can intrude and use their access to obtain sensitive information, commit identity theft, disrupt operations, or launch attacks against other computer systems and networks.

To maintain the security of its computer systems, the Department has implemented an Information Security Policy that requires all its information be protected from unauthorized access. The policy applies to all Department information systems and communication networks as well as the information stored, processed, and produced on or by these systems and networks. The policy outlines the responsibilities of all users of the information systems to maintain the security of the systems and to safeguard the confidentiality of Department information. The policy also provides staff with an understanding of the vulnerabilities and risks associated with information security and the appropriate steps to be taken to protect information resources.

The Department's internal network interconnects its computer systems to the main Education Building and Education Building Annex sites as well as the Cultural Education Center in Albany and approximately 40 satellite office locations throughout the State. As of February 2017, the Department had 2,450 employees with network access.

Audit Findings and Recommendations

While the Department has implemented numerous information security controls to protect its critical systems and data, weaknesses exist that place the confidentiality, integrity, and availability of the systems and information at risk. For example, the Department has not performed a complete data classification analysis and an inventory of assets associated with its critical systems and sensitive data. It also has not established adequate policies and procedures to secure its critical information systems. Furthermore, the Department also needs to improve its disaster recovery planning procedures to better ensure the availability of critical systems in the event of a disaster.

As a result of our audit, the Department plans to take various actions to bolster its security over critical systems, including improving certain aspects of its information security program and addressing the technical issues that we identified during our audit. Until the Department takes these steps, however, its critical systems will continue to be at risk.

Information Security Program

Strong information security programs establish a framework for assessing risk, developing and implementing effective security procedures, and monitoring the effectiveness of these procedures. They also incorporate methods to remediate information security weaknesses and periodically test security response plans. Effective controls can help ensure that only authorized users (people and processes) access information and systems to lessen the chances of unauthorized disclosures of information, improper changes or modifications to information and systems, and system disruptions that could hamper the Department's ability to perform its mission.

The Department has taken various proactive measures to protect its critical systems and data. For example, in early 2016, the Department contracted with a vendor to perform both an internal and external security assessment of their information systems. Also, the Department has adopted various information security policies and procedures covering multiple information security components, including incident response, acceptable use of information technology resources, password guidelines, mobile device security, and contingency planning. However, as explained in the following sections, the Department has not implemented key components of an information security program. Unless the Department improves its overall information security program, its critical systems and data will remain vulnerable to unauthorized access and/or service disruption.

Data Classification

All information, whether in printed or electronic form, should be classified and labeled in a consistent manner to ensure data confidentiality, integrity, and availability. The data classification process assigns a level of risk to various types of information, which helps management make appropriate decisions about the level of security the data requires. Currently, the Department operates 120 computer systems to help support its activities. This includes four systems deemed critical to Department operations that we focused our testing on. Each of the four systems

supports crucial Department services to the general public and contains sensitive personal data and student records. Besides these four systems, 30 other Department systems contain similar sensitive personal data and/or student records protected under the Family Educational Rights and Privacy Act (FERPA).[1]

Despite the sensitive data its computer systems process and store, the Department has not completed a full data classification of all agency information. Additionally, the Department does not have a complete inventory of its information technology assets, such as hardware and software, which are used to access Department systems and data. Unless the Department classifies the data it maintains, sets and enforces appropriate security levels for the data, inventories where the data resides, and updates the classification and inventory on an ongoing basis, it cannot ensure that the appropriate level of security controls is applied to the sensitive data handled by its critical systems.

Department officials acknowledged that data classification is an important first step in creating a strong security program. According to officials, the Department had previously initiated data classification, but it was never completed, and recent efforts have been made to seek appropriate resources to plan and undertake a thorough data classification project. Officials indicated that once the data and the systems that manage data are classified, the Department can account for the associated hardware and software that support critical systems and then better implement the appropriate security controls. By taking such steps, the Department can better ensure the confidentiality, integrity, and availability of its critical systems.

Security Policy and Procedures

Risk-based policies, procedures, and technical standards that govern the security of an entity's computing environment are key to an effective information security program. Properly developed, documented, and implemented, such policies and procedures should help reduce the risk associated with unauthorized access and/or disruption of services. Security policies are the primary mechanisms by which management communicates its views and requirements, and also serve as the basis for adopting specific procedures and technical controls. Technical security standards can provide consistent implementation guidance for each computing environment. In addition, entities need to take the actions necessary to effectively implement or execute these procedures and controls. Otherwise, critical systems and their associated data will not receive the protection that the security policies and controls should provide.

Although the Department has adopted various information security policies and procedures covering multiple information security components, we noted instances in which formal procedures had not been developed for key information security program elements, including, but not limited to:

---

[1] FERPA requires written permission from the parent or the student to release information from the student's education record to any party, except in limited circumstances identified by statute.

- Wireless deployment;
- Vulnerability management;
- Patch management;
- Secure software development;
- Payment card industry (PCI) security standards; and
- Physical controls over computer equipment.

Department officials acknowledged that there are many policies that need to be developed. Further, they indicated the Department does have several policies and procedures currently in draft stage, including a PCI security standards policy. While information security and procedures policies do not guarantee the security of the Department's critical systems, the lack of policies significantly increases the risk that system data may be subject to inappropriate access or use.

Disaster Recovery

A strong system of information security controls includes a disaster recovery plan (DRP), which describes how an organization will deal with potential disasters – that is, any sudden, unplanned catastrophic event such as a fire, flood, computer virus, vandalism, or inadvertent employee action that compromises the integrity of computer systems and their associated data. Further, it is important that the DRP be tested periodically and updated to address changes in security requirements.

While the Department does have a DRP, we determined it is incomplete and outdated. For example, the Department's own process states that the DRP should contain an Emergency Response Plan (ERP) that proactively defines the appropriate information technology measures to be taken in response to specific types of emergencies. However, we found that the Department never developed a formal ERP. This is particularly significant considering the Department does not have an alternative disaster recovery site to support and restore critical applications to full capacity when a disaster causes a system outage.

The lack of an ERP and alternative disaster recovery site increases the likelihood that the Department could suffer serious interruptions in its critical systems, affecting not only Department system users but public users as well. For example, local school districts might be unable to use fingerprinting and background check functionalities to validate applicants during the hiring process, or licensed professionals could be prevented from practicing their trade for an unknown amount of time. The Department would have to revert to paper operations for verification purposes, which could delay the professional from receiving their license to practice.

Furthermore, although the DRP is required to be updated and tested at least annually, the Department's DRP has not been fully updated since 2013 or tested since 2011. Officials attributed this to a variety of factors, including limited resources and a focus on higher-priority projects. They indicated, however, that the Department is developing a new disaster recovery strategy to ensure adequate mission-critical system support can be provided in the event of a disaster, and that significant changes are being considered, such as opportunities for co-location of architecture and cloud-based backup.

Recommendation

1. Develop strategies to enhance security controls over critical systems. This should include, but not be limited to:

   - Adopting and adhering to policies and procedures that address all aspects of information security, including procedures covering the classification of data and other areas identified as lacking procedures;
   - Completing the DRP enhancement efforts to better ensure adequate mission-critical system support in the event of a disaster; and
   - Updating and testing the DRP at least annually.

Technical Controls

During our testing, we identified technical IT controls that need to be corrected to ensure the Department's critical information systems and their associated data are not at risk. Due to their confidential nature, we reported these matters to officials in a separate report and, consequently, do not address them in detail in this report. In response to our preliminary findings, officials stated the Department has since fixed certain technical weaknesses that we reported, and it will take other actions to improve technical controls over its critical systems.

Recommendation

2. Implement the recommendations detailed during the audit to strengthen technical controls over critical systems.

Audit Scope, Objective, and Methodology

The objective of our audit was to determine whether the security controls over critical Department information systems were sufficient to minimize the various risks associated with unauthorized access to these systems and their associated data. Our audit scope covers the period September 29, 2016 through March 30, 2017.

To accomplish our objective, we met with staff from multiple Department program units to identify critical applications and the information systems that support them. We also interviewed agency technical staff responsible for network security and operations to determine how these applications are accessed over the Department's networks. In addition, we reviewed policies and procedures that we deemed important to the control and maintenance of critical system security. We also examined records and reports pertinent to our audit scope. We tested security controls to assess the internal controls over critical systems, including the risk of unauthorized access to the systems. We also made physical observations of the hardware and network devices supporting critical systems.

We conducted our audit in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objective. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objective.

In addition to being the State Auditor, the Comptroller performs certain other constitutionally and statutorily mandated duties as the chief fiscal officer of New York State. These include operating the State's accounting system; preparing the State's financial statements; and approving State contracts, refunds, and other payments. In addition, the Comptroller appoints members to certain boards, commissions, and public authorities, some of whom have minority voting rights. These duties may be considered management functions for purposes of evaluating threats to organizational independence under generally accepted government auditing standards. In our opinion, these functions do not affect our ability to conduct independent audits of program performance.

Authority

The audit was performed pursuant to the State Comptroller's authority as set forth in Article V, Section 1 of the State Constitution and Article II, Section 8 of the State Finance Law.

Reporting Requirements

We provided a draft copy of this report to Department officials for their review and formal comment. We considered their comments in preparing this report and attached them in their entirety at the end of it. Officials agreed with our findings and recommendations, and indicated they will address our recommendations and continue to take steps to improve the Department's information security program.

Within 90 days after final release of this report, as required by Section 170 of the Executive Law, the Commissioner of the State Education Department shall report to the Governor, the State Comptroller, and the leaders of the Legislature and fiscal committees, advising what steps were taken to implement the recommendations contained herein, and where recommendations were not implemented, the reasons why.

Contributors to This Report

Brian Reilly, CFE, CGFM, Audit Director
Nadine Morrell, CIA, CISM, CGAP, Audit Manager
Mark Ren, CISA, Audit Supervisor
Holly Thornton, CFE, Examiner-in-Charge
Jared Hoffman, OSCP, GPEN, GWAPT, Information Technology Specialist
Christopher Bott, Senior Examiner
Rachael Hurd, Senior Examiner
Mary McCoy, Senior Editor

Division of State Government Accountability

Andrew A. SanFilippo, Executive Deputy Comptroller
518-474-4593, asanfilippo@osc.state.ny.us

Tina Kim, Deputy Comptroller
518-473-3596, tkim@osc.state.ny.us

Brian Mason, Assistant Comptroller
518-473-0334, bmason@osc.state.ny.us

Vision

A team of accountability experts respected for providing information that decision makers value.

Mission

To improve government operations by conducting independent audits, reviews and evaluations of New York State and New York City taxpayer financed programs.

Agency Comments

THE STATE EDUCATION DEPARTMENT / THE UNIVERSITY OF THE STATE OF NEW YORK / ALBANY, NY 12234

DEPUTY COMMISSIONER
Office of Performance Improvement and Management Services
O: 518.473-4706
F: 518.474-5392

June 5, 2017

Mr. Brian Reilly
Audit Director
Division of State Government Accountability
Office of the State Comptroller
110 State Street – 11th Floor
Albany, NY 12236-0001

Re: Response to Draft Report 2016-S-69 SED

Dear Mr. Reilly:

The following is the response of the New York State Education Department (the Department) to the Draft Report, 2016-S-69 SED Security Over Critical Systems.

<u>Recommendation 1</u>:

Develop strategies to enhance security controls over critical systems. This should include, but not be limited to:

- Adopting and adhering to policies and procedures that address all aspects of information security, including procedures covering the classification of data and other areas identified as lacking procedures.

- Completing the DRP enhancement efforts to better ensure adequate mission-critical system support in the event of a disaster.

- Updating and testing the DRP at least annually.

<u>Response</u>:

We appreciate the auditor's recognition that 'the Department has implemented numerous information security controls to protect its critical systems and data'. We also appreciate the auditor's recognition of the Department's prior and ongoing efforts toward the betterment of Department information security controls, including such policies, procedures, data classification, and disaster recovery planning (DRP), amongst others.

It is the Department's belief that since establishing a dedicated information security office (approximately 2 1/2 years ago), we have made great progress in developing a comprehensive information security program. Many of the auditor's findings were immediately acknowledged by the Department as the audit progressed, because most of the findings were already identified by the Department as areas of needed improvement in the program. We therefore agree that there

is more work to be done to improve the program and that more resources will be needed to complete such work expeditiously.

The Department intends to address Recommendation 1 through:

- Establishing an Information Governance program, with representative stakeholders from each of the Department's program offices, to catalog and classify Department data.

- Continuing to develop new information security policies and procedures (including those that the Department currently has in draft, and those of which were identified as 'noted instances' by the auditor) and processing their approval up through the Department's IT Policy Lifecyle.

- Finishing the current 2017 update of the Department's existing Disaster Recovery Plan (DRP) to reflect the Department's current computing environment, and distributing the updated plan (and continue to do so annually, as described in the plan). Further, applying such significant changes as the architecture co-location and cloud-based backup opportunities that are currently being explored, when implemented. Further, testing the plan to ensure its effectiveness and making any necessary adjustments to meet the plans goals.

Recommendation 2:

Implement the recommendations detailed during the audit to strengthen technical controls over critical systems.

Response:

As described in the audit, 'due to their confidential nature we (the auditor) reported these matters to (Department) officials in a separate report'.

The Department has reviewed this separate report and we agree with the recommendations stated therein. The Department has provided the auditor with responses to the separate report.

If you have any questions regarding this response, please contact Thalia Melendez, Director of Audit Services (518) 473-4516.

Sincerely,
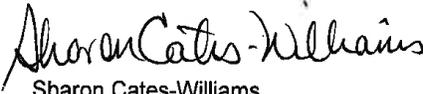
Sharon Cates-Williams

c: Thalia Melendez
   Karen Starke
   Tope Akinyemi
   Edward Skinner