THOMAS P. DiNAPOLI
COMPTROLLER

110 STATE STREET
ALBANY, NEW YORK 12236

STATE OF NEW YORK
OFFICE OF THE STATE COMPTROLLER

November 13, 2018

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

Re: Security Over Critical Information Systems
Report 2018-F-17

Dear Commissioner Elia:

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, we have followed up on the actions taken by officials of the State Education Department to implement the recommendations contained in our audit report, *Security Over Critical Information Systems* (Report 2016-S-69).

Background, Scope, and Objectives

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. 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.

To help carry out its responsibilities, the Department operates 120 computer systems. Our original audit focused on four systems that were deemed critical to the Department's operations. 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 ensuring the confidentiality, integrity, and availability of its systems.

Our initial audit report, which was issued on July 19, 2017, determined 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. The audit covered the period September 29, 2016 through March 30, 2017. We determined that,

although the Department had taken a number of steps to secure its critical information systems and associated data, there was still a risk that unauthorized persons could access these systems. We found the Department had not taken fundamental steps to secure its critical systems, such as completing a full data classification process, adopting adequate information security policies and procedures, and improving certain technical controls over its critical systems.

The objective of our follow-up was to assess the extent of implementation, as of November 1, 2018, of the two recommendations included in our initial audit report.

Summary Conclusions and Status of Audit Recommendations

The Department has not made significant progress in implementing the recommendations identified in our initial audit report. Of the two prior audit recommendations, one has been partially implemented, and one has been not been implemented.

Follow-Up Observations

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 Disaster Recovery Plan enhancement efforts to better ensure adequate mission-critical system support in the event of a disaster; and*
- *Updating and testing the Disaster Recovery Plan at least annually.*

Status - Not Implemented

Agency Action - As of November 2018, the Department has not yet adopted policies and procedures to address all aspects of information security, nor has it completed enhancements to its disaster recovery plan to ensure mission-critical systems are supported or updated and tested its disaster recovery plan. Department officials attribute much of the lack of progress to a vacancy in the Chief Information Security Officer (CISO) position since September 2017. The CISO is responsible for developing and implementing information security policy. Once a CISO is in place, the Department expects to formally adopt policies that are currently in draft form, and update its disaster recovery capabilities along with its plan. We encourage the Department to implement our recommendation soon after a CISO is in place.

Recommendation 2

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

Status - Partially Implemented

Agency Action - During our initial audit, we issued a preliminary report and a confidential draft report to the Department. The reports contained a total of five recommendations. Our review found that, of the five recommendations, one has been implemented, one has been partially implemented, and three have not been implemented.

Major contributors to this report were Brian Krawiecki, Holly Thornton, Christopher Bott, and Charles Lansburg.

We would appreciate your response to this report within 30 days, indicating any actions planned to address the unresolved issues discussed in this report. We thank the management and staff of the State Education Department for the courtesies and cooperation extended to our auditors during this review.

Very truly yours,

Nadine Morrell, CIA, CISM
Audit Manager

cc: Karla Ravida, Audit Liaison