December 13, 2018

Nadine Morrell
Audit Manager
Division of State Government Accountability
Office of the State Comptroller
110 State Street – 11th Floor
Albany, NY 12236

Dear Ms. Morrell:

The following is the New York State Education Department's (Department) response to the audit report, 2018-F-17; Security Over Critical Information Systems, which is a follow-up report on actions taken by the Department as a result of the audit report 2016-S-69.

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.

While the Department has operational security measures, policies and procedures in place to protect its information assets, it recognizes that there is room for improvement. The Chief Information Security Officer (CISO) position, which has been vacant for more than a year, has recently been filled and the new CISO is anticipated to start work on December 27, 2018. The CISO is responsible for the Department's information security program, and the review, development and updating of the Department's information security related policies and procedures will be prioritized to ensure the Department is quickly brought into compliance with the audit recommendations.

Regarding the disaster recovery plan, the Department is currently engaged in a major technology refresh. For example, the Department continues to invest in improvements to its backup and recovery systems and overall resiliency and is actively exploring the establishment of a standby site. These changes have already rendered much of the current disaster recovery plan moot. When the planned initiatives are complete, the Department will revise the disaster recovery plan to reflect the new system environment, and testing and updating of the plan as needed, will follow.

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

Status: Partially Implemented

As described in the initial audit, a preliminary and a confidential draft report were issued to the Department. The Department has discussed the details of the recommendation 2 as they relate to the follow-up with the auditors.

The Department has provided a separate response to the audit manager with responses to the confidential portion of the report.

Yours truly,

Sharon Cates-Williams
Deputy Commissioner

cc: Karla Ravida
     Tope Akinyemi
     Jeff Deal