October 17, 2017

Hon. Thomas P. DiNapoli
New York State Comptroller
110 State Street, 15th Floor
Albany, NY 12236

Dear Comptroller DiNapoli:

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

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.

- Updating and testing the DRP at least annually.

Response:

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. A proposal to conduct a data classification project is currently under development.

- 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. Since the audit was conducted, several policies have been drafted and are currently in the review process.

- Updating the Department's existing Disaster Recovery Plan (DRP) to reflect the Department's current computing environment and changes in staffing. The updated plan will be distributed and updated at least annually, as described in the plan. Significant changes to the architecture currently being researched, such as co-location and cloud-based systems, will be included if implemented. The DRP will be tested to ensure its effectiveness and to identify any necessary adjustments to meet the plan's goals. Improvements in the Department's offsite backup capabilities are being designed, and will be implemented as soon as possible.

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.

Yours truly,

Sharon Cates-Williams

Deputy Commissioner

Sharon Cates-Williams

cc: Brian Reilly
    Thalia Melendez
    Karen Starke
    Tope Akinyemi