New York State Comptroller
THOMAS P. DiNAPOLI

Privacy and Security of Student Data

State Education Department

Report 2021-S-29 | **May 2023**

Spotlight on Education

Audit Highlights

Objectives

To determine if the State Education Department (Department) consistently follows all laws and regulations regarding the safety and privacy of students' data and is monitoring New York State school districts to ensure they are complying with the legislation and regulations that govern data privacy and security. The audit covered the period from March 2020 through November 2022.

About the Program

The Department is part of the University of the State of New York, one of the most complete, interconnected systems of educational services in the United States. 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 2.4 million students. The Department is responsible for safeguarding its data and ensuring the confidentiality, integrity, and availability of its systems.

The COVID-19 pandemic forced many schools across the nation to close in 2020 and quickly transition to a remote learning environment, leading to an increased reliance on technology. This resulted in an escalation of cybersecurity threats – including ransomware and other types of cyberattacks. According to a U.S. Government Accountability Office report, the number of students impacted by cyberattacks rose from 39,000 students in 2018 to a high of nearly 1.2 million students in 2020. It is, therefore, more important than ever to ensure that schools have secure systems that protect the safety and privacy of students and their data.

In 2020, the Department adopted Part 121 of the Regulations of the Commissioner of Education (Part 121), which implements Section 2-d of the Education Law and outlines numerous requirements that all schools must implement to strengthen data privacy and security and protect personally identifiable information (PII). Our audit focused on charter schools and school districts, collectively referred to as school districts in this report.

Key Findings

- The Department did not provide adequate oversight of school districts' compliance with the notification requirements for data incidents.
- The Department did not provide sufficient oversight of school districts' compliance with other key requirements of Part 121.
- The Department has not completed a data classification for all the types of information it manages, processes, or stores, some of which contain student PII.
- We identified weaknesses in technical controls that need to be corrected to ensure the selected Department and school district information systems and their associated data are not at risk.

Key Recommendations

- Develop and implement controls to monitor school districts' compliance with Part 121.
- Continue to work on completing a full data and asset classification of all current Department systems and data.
- Implement the recommendations detailed in the preliminary report to strengthen technical controls over the selected systems reviewed.

Office of the New York State Comptroller
Division of State Government Accountability

May 16, 2023

Betty A. Rosa, Ed.D.
Commissioner
State Education Department
State Education Building
89 Washington Avenue
Albany, NY 12234

Dear Dr. Rosa:

The Office of the State Comptroller is committed to helping State agencies, public authorities, and local government agencies manage their resources efficiently and effectively. By so doing, it provides accountability for the 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 *Privacy and Security of Student Data*. This audit was performed pursuant to the State Comptroller's authority under 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,

Division of State Government Accountability

Contents

Glossary of Terms

Term	Description	Identifier
Department	State Education Department	*Auditee*
BOCES	Boards of Cooperative Educational Services	*Key Term*
CPO	Chief Privacy Officer	*Key Term*
DPO	Data Protection Officer	*Key Term*
NIST CSF	National Institute for Standards and Technology Cybersecurity Framework	*Key Term*
Parents' Bill of Rights	Parents' Bill of Rights for Data Privacy and Security	*Key Term*
Part 121	Part 121 of the Regulations of the Commissioner of Education	*Law*
PII	Personally identifiable information	*Key Term*
RIC	Regional Information Center	*Key Term*

Background

The COVID-19 pandemic forced schools across the nation to close in 2020, with teachers and students quickly transitioning to a remote learning environment. Remote or hybrid education increased the reliance on technology to deliver educational services, resulting in an escalation of cybersecurity threats – including ransomware and other types of cyberattacks. According to a U.S. Government Accountability Office report, the number of students impacted by cyberattacks rose from 39,000 students in 2018 to a high of nearly 1.2 million students in 2020. It is, therefore, more important than ever to ensure that schools have secure systems that protect the safety and privacy of students and their data.

The State Education Department (Department) is part of the University of the State of New York, one of the most complete, interconnected systems of educational services in the United States. 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 2.4 million students, 12 Regional Information Centers (RICs), and 37 Boards of Cooperative Educational Services (BOCES). The BOCES and RICs work to provide shared educational programs and services to schools throughout the State and host various schools' student information systems and the student data reporting processes. The Department operates 120 computer systems to help support its activities and is responsible for safeguarding its data and ensuring the confidentiality, integrity, and availability of its systems.

The Department is charged with the general management and supervision of all public school districts and all the educational work of the State. It is also responsible for ensuring compliance with relevant laws and regulations, including Section 2-d of the Education Law (Education Law § 2-d) and Part 121 of the Regulations of the Commissioner of Education (Part 121), which was adopted in January 2020. Education Law § 2-d requires the Commissioner of Education to establish standards for data security and privacy policies, which shall include, but not be limited to:

- Data privacy protections;
- Data security protections, including data systems monitoring;
- Data encryption;
- Incident response plans;
- Limitations on access to personally identifiable information (PII)[1];
- Safeguards to ensure PII is not accessed by unauthorized persons when transmitted over communication networks; and
- Application of all such restrictions, requirements, and safeguards to third-party contractors.

1 PII is any information that could identify a specific individual, including, but not limited to, the name or address of a student, parent, or family member; a personal identifier, such as a student number; an indirect identifier, such as date of birth; or other information that alone or in combination could identify a student.

In accordance with Education Law § 2-d, Part 121 further strengthens data privacy and security by requiring schools to adopt and publish a data security and privacy policy that implements the requirements of Part 121 and aligns with the National Institute for Standards and Technology Cybersecurity Framework (NIST CSF) by October 2020. The NIST CSF is a comprehensive framework designed to assist user organizations in establishing and improving their cybersecurity program to reduce vulnerabilities. Part 121 also stipulates requirements for reporting and notification of breaches or the unauthorized release of PII. Schools are further required to designate a Data Protection Officer (DPO) to implement the policies and procedures required in Education Law § 2-d and Part 121 and serve as the point of contact for data security and privacy issues. Finally, Part 121 requires schools to post on their website a Parents' Bill of Rights for Data Privacy and Security (Parents' Bill of Rights) and a supplement to the Parents' Bill of Rights for any contract or written agreement with a third-party contractor that received PII. These supplements detail the purposes for which student data will be used by the third-party contractor, the duration of the contract, and a general overview of how the data will be stored and protected.

Audit Findings and Recommendations

The increased relevance of safe and secure technology in the education system brought about by the pandemic makes it especially important that the Department be proactive in ensuring the protection of its data and systems. Our audit focused on charter schools and school districts, collectively referred to as school districts for this report. We found that the Department did not fully comply with its policies related to information security and data privacy, nor did it provide sufficient oversight of school districts to ensure compliance with key requirements of Part 121, such as security policies, incident reporting, and the Parents' Bill of Rights. Given the magnitude of cybersecurity breaches involving PII, the Department should ensure school districts have taken all the required steps outlined within Part 121 to best protect student data. Further, the Department has not taken the fundamental steps or improved the technical controls needed to secure its own critical systems. It has not completed a data classification for all types of information that it creates, collects, processes, or stores, some of which contain student PII. If systems have not been properly classified, they may lack the appropriate security controls to protect student data. In addition, we identified weaknesses in technical controls that need to be corrected to ensure the selected Department and school district information systems and their associated data are not at risk. Due to their confidential nature, we provided detailed technical reports to school district officials and reported certain other matters to Department officials in separate reports.

Implementation of Part 121 Requirements

Insufficient Reporting of Data Incidents

Data incidents, or breaches, are the unauthorized acquisition, access, use, or disclosure of student, teacher, and/or principal data. Any data incident must be reported by the affected school district to the Department's Chief Privacy Officer (CPO) using a form available on the Department's website. The audit team requested and reviewed supporting documentation for the 131 data incidents reported at school districts for the period March 2020 through April 2021. We determined that many of the reports were incomplete or missing, with the Department unable to provide supporting documentation for nine data incidents. Due to the missing information, the Department cannot confirm if affected parties were notified of the data incident.

Of the 131 data incidents, 55 (42%) were missing one of the following required dates in the reporting form: date of incident, date of discovery, or date of notification to affected parties. Without the required information, the Department was unable to determine whether school districts met the reporting deadlines, as defined in Part 121, or in some cases even contacted the affected parties. Additionally, the number of data incidents provided was inconsistent with the number that the Department reported in its Annual Report on Data Privacy and Security. For example, the 2020 Annual Report cited 44 data incidents for calendar year 2020; however, for the period March 2020 through December 2020 alone, we were provided reports for 57 data incidents. When we presented this information to Department officials in our preliminary report, officials did not directly address this finding.

With the rise of cyberattacks, the timely communication of suspected information breaches is especially important. To this end, Part 121 specifies time frames for the notification of all affected parties of a breach or unauthorized release of information. When a school district discovers a breach or an unauthorized release of information, it has 10 days to notify the Department's CPO of the data incident. Of the 131 data incidents, 39 (30%) exceeded the 10-day maximum from the date of discovery. For an additional 18 incidents (14%), the Department did not have enough information to determine whether the 10-day maximum was exceeded due to missing forms or incomplete forms that did not specify an exact date when the school district notified the Department. Further, as required by Part 121, school districts must notify affected parties within 60 calendar days after the discovery of a breach or unauthorized release. For 52 of the 131 data incidents (40%), the school district did not provide the specific date of notification to affected parties to determine if they were timely. Department officials did not always follow up with the school districts to determine if affected parties were notified. Due to the nature in which data incidents and responses occur, and the manner in which the Department tracks reported data incidents, we found school districts may not be able to report all of the information in a single data incident report, and there is no formal process that allows for updates from the school districts.

The Department should ensure school districts notify it of all data incidents. In addition, the Department should ensure that notification is made to affected parties and in compliance with the time frames established in Part 121. Without accurate reporting and tracking of data incidents, the Department cannot ensure appropriate actions are taken to address the breach or unauthorized release of student data or that the affected parties are notified.

Security Policies and Data Protection Officers

Part 121 further outlines numerous requirements that all school districts must implement to strengthen data privacy and security and protect PII. Some of the key requirements include adopting and publishing a data security and privacy policy that incorporates the NIST CSF by October 1, 2020 and posting on their website a Parents' Bill of Rights and a supplement to the Parents' Bill of Rights for any contract or written agreement with a third-party contractor that received PII. We reviewed the websites of a sample of 169 school districts and found numerous instances of non-compliance with Part 121.

Of the 169 websites we reviewed, as of March 2022, 52 (31%) did not have a data security and privacy policy. In addition, of the 117 school districts that posted their data security and privacy policy, 35 did not meet the October 1, 2020 deadline and 16 did not have an adoption date in order to verify meeting the deadline. Moreover, four school districts had policies that were adopted before the deadline, but the policies did not comply with the requirements of Part 121. We also identified 25 school districts (15%) that were missing the Parents' Bill of Rights and 73 (43%) that failed to post the supplement to the Parents' Bill of Rights for any third-party contracts. Further, we were unable to contact 11 school districts that were missing

either the Parents' Bill of Rights or the data security and privacy policy (seven were missing both requirements). Of these 11 school districts, three had previously reported a data incident, which, according to Department officials, prompts an informal review of their website. However, the Department did not have any documentation of these reviews. An informal review by the Department should have identified that the required postings were missing and directed the school districts to correct their websites and/or policies. As a result of our audit work, two school districts added the Parents' Bill of Rights to their website and two are in the process of adding missing information. It is important that parents, students, and staff have this information readily available to understand the requirements for data security, steps that should be taken when protecting student data, and their rights under the law.

To ensure school districts have a central point of contact to oversee the implementation of the policies and procedures specified in Education Law § 2-d and Part 121, each school district is required to designate a DPO. The Department maintains a spreadsheet of school districts' DPO information, which is accessible via a Public Reports Portal on the Department's website – a platform the Department uses to publish institutional information for transparency and public use. In our sample of 169 school districts, 14 did not have a DPO. Our review of the Department's DPO spreadsheet for our sample of 169 school districts found that for seven school districts the email addresses listed were incorrect and the DPOs were thus unreachable; for eight others, the DPO listed on the Department's spreadsheet was not the same individual identified on the school district's website. The DPO is not only responsible for the implementation of policies and procedures required under Education Law § 2-d and Part 121 but also serves as the point of contact for data security and privacy issues for the school district. A DPO is required and essential for school districts, and accurate contact information should be readily available. Further, without an accurate list of DPOs, the Department cannot be assured that information regarding student data privacy and security will reach the appropriate representative from each school district.

Site Visits

To assess the guidance and oversight provided by the Department related to the implementation of Part 121, we met with the administration and technology department officials of 16 school districts. Officials at 13 of the 16 (81%) stated they did not receive any guidance regarding the implementation of the new Part 121 from the Department. In addition, officials at 14 of the 16 (88%) stated that the Department has not requested or required them to submit their data security and privacy policy or the Parents' Bill of Rights. The other two school districts were unable to recall if the Department had requested them.

Additionally, according to Part 121, school districts are required to provide annual data privacy and security awareness training to all employees with access to PII. Of the 16 school districts we visited, three do not provide specific data privacy and security awareness training to employees.

Further, during four site visits at school districts that host their student information systems, we conducted vulnerability scans that identified weaknesses in their systems. These school districts had not performed any testing of their systems, even though it is required by NIST CSF. The results of the scans are confidential in nature and therefore are not detailed in this report. However, the results were provided to school district officials, who took immediate actions to remediate the vulnerabilities identified. The Department relies on the local BOCES and RICs to provide direct assistance to school districts to ensure they are complying or meeting the requirements of Part 121, including implementation of the applicable provisions of the NIST CSF as they relate to an individual school district. However, if the Department is not monitoring school district compliance with and implementation of Part 121 or common vulnerabilities, this affects its ability to issue relevant and impactful guidance to the school districts, as needed.

In response to our preliminary findings, Department officials agreed that transparency to parents and students regarding data privacy and security policies is of the utmost importance, especially now that school districts are using more educational technology tools than ever. They further stated that competing priorities and the loss of staff within the Department's Privacy Office prevented the initiation of a formal monitoring program. However, Department officials agreed with our findings and, as a result, they intend to develop a protocol to monitor school district compliance with Part 121 in the first half of 2023 and begin monitoring compliance in the second half of 2023. They further noted that they increased engagement with the field, including with those providing services to the school districts such as the BOCES and the RICs.

Department Security Controls

Incomplete Data Classification

Data classification is the basis for identifying an initial baseline set of security controls for data, data systems, and evaluation of retention and disposition schedules. According to the Department's Information Security Policy, all data – both electronic and non-electronic, which includes student, teacher, and administrator PII – must be assigned a classification level based on the potential impact to the Department should certain events occur that interfere with the data or the systems needed to accomplish its assigned mission, responsibilities, and asset protection. This classification must be reviewed on an ongoing basis. The Department's Data Classification Policy, in place since October 2020, established the data classification process for protecting the confidentiality, integrity, and availability of all data the Department produces or is the custodian of – both public and internal, written and electronic. If data and systems have not been properly classified, they may lack the appropriate security controls.

Despite having systems that process and store student PII and the data classification requirement being in place, the Department has not completed a full data classification of its information. In addition, this was noted in a previous audit

performed by this office, *Security Over Critical Information Systems* (2016-S-69), issued July 19, 2017. Further, during our follow-up review (2018-F-17), issued November 13, 2018, we found that the Department had not made significant progress in implementing our recommendations, and its data still had not yet been classified.

Department systems capturing, storing, or otherwise processing sensitive data that has not been classified could lack the appropriate security controls and potentially be accessed for unauthorized purposes or by unauthorized individuals. In the case of an information security incident, the Department may be unable to identify in a timely manner what, if any, sensitive and/or critical data was involved and may be compromised.

According to Department officials, turnover of relevant executive staff in the Information Security Office slowed the data classification process. However, during the audit, in the first quarter of 2022, the Department began the process of data classification by contracting with the New York State Technology Enterprise Corporation and working with various Department program areas. This has an estimated completion date of February 2023, which is 5½ years after our initial audit.

Weaknesses in Technical Controls

During our testing, we identified systems containing student PII not maintained at vendor-supported levels and weaknesses in technical controls that need to be corrected to ensure the selected Department information systems and their associated data are not at risk. Due to their confidential nature, we disclosed these matters to Department officials in a separate report and, consequently, do not address them in detail in this report. In response to our preliminary report, officials stated the Department has since addressed certain issues we identified and has begun to take steps to implement the remaining recommendations.

Recommendations

1. Develop and implement controls to monitor school districts' compliance with Part 121.
2. Continue to work on completing a full data and asset classification of all current Department systems and data.
3. Implement the recommendations detailed in the preliminary report to strengthen technical controls over the selected systems reviewed.

Audit Scope, Objectives, and Methodology

The objectives of our audit were to determine if the Department consistently follows all laws and regulations regarding the safety and privacy of students' data and is monitoring New York State school districts to ensure they are complying with the legislation and regulations that govern data privacy and security. The audit covered the period from March 2020 through November 2022.

To accomplish our objectives and assess related internal controls, we reviewed relevant laws, regulations, and guidance. We interviewed Department officials to gain an understanding of their efforts to monitor compliance with the requirements of Part 121. We also interviewed officials from multiple Department program units to identify systems that handle student data. In addition, we reviewed policies and procedures that we deemed important to the control and maintenance of these systems. Further, we reviewed records and reports related to data incidents.

To determine school districts' compliance with certain elements of Part 121, we selected a stratified random sample of 130 from a population of 1,667 (2,621 school districts less New York City and out-of-state schools) based on the following strata: school districts, BOCES, non-public schools, other schools serving students with disabilities, approved preschool programs, and public charter schools. We combined this with the initial list of school districts that reported a data incident for a total of 257 schools. After removing duplicates and schools that do not fall under Part 121 requirements, we reviewed a total of 169 school district websites. Of the 169 school districts, we selected a judgmental sample of 16 schools to interview and gain an understanding of their practices related to their implementation of Part 121 requirements and the guidance and oversight provided by the Department. These school districts were selected based on geographic location within the State, how their student data is stored, Part 121 compliance, prior data incidents reported, and size. We also performed vulnerability scans at four of these school districts that hosted their student information systems and had not performed their own scans. In addition, we reviewed the results of vulnerability scans of some Department systems that contained student PII. The samples were not projected or intended to be projected across the population. We determined that the data used to pull our samples and perform our analysis was sufficiently reliable for our use in accomplishing our audit objectives.

Statutory Requirements

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.

We conducted our performance 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 objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

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. These duties could be considered management functions for purposes of evaluating organizational independence under generally accepted government auditing standards. In our professional judgment, these duties do not affect our ability to conduct this independent performance audit of the Department's oversight and administration of school districts to ensure they are complying with the legislation and regulations that govern data privacy and security.

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 final report and have included them in their entirety at the end of it. In their response, Department officials agreed with our audit conclusions and recommendations and indicated that actions have been and will be taken to address them.

Within 180 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.

Agency Comments

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

EXECUTIVE DEPUTY COMMISSIONER
(518) 473-8381
E-mail: Sharon.Cates-Williams@nysed.gov

March 23, 2023

Ms. Nadine Morrell
Audit Director
Division of State Government Accountability
110 State Street, 11th Floor
Albany, NY 12236-0001

Re: Draft Audit Report 2021-S-29, Issued February 24, 2023

Dear Ms. Morrell:

The New York State Education Department (Department) provides the following response to the Office of the State Comptroller's (OSC) draft audit of the *New York State Education Department – Privacy and Security of Student Data* (2021-S-29).

Part 121 of the regulations of the Commissioner of Education became effective just over three years ago, on January 29, 2020. This was also less than two months before the pandemic kept students from attending school in person and required schools to pivot to on-line learning for all classes. These regulations clarify the data privacy and security obligations of educational agencies and third-party contractors; establish requirements for contracts and other written agreements where personally identifiable information (PII) will be provided to a third-party contractor; establish the National Institute of Standards and Technology (NIST) Cybersecurity Framework as the standard for educational agencies data security and privacy programs; require educational agencies to provide annual data security and privacy training to its officers and employees; and require that educational agencies identify a data protection officer (DPO) who will be responsible for the educational agency's data privacy and security program.

As stated in the draft report, the Department agrees that transparency to parents and eligible students regarding educational agencies' policies ensuring the privacy and security of student data is of the utmost importance—especially when schools are using more educational technology tools than ever before.

OSC Recommendation 1:

"Develop and implement controls to monitor school districts' compliance with Part 121."

Department's Response:

Although Part 121 is relatively new, monitoring educational agencies for compliance with Part 121 of the regulations of the Commissioner of Education has been, and remains, one of the goals of the Department's Privacy Office. That goal, however, exists alongside several other priorities the Privacy Office has established since January 2022, including building the trust of educational agencies through continued outreach; forming a data privacy advisory committee; issuing required documents (e.g., parent complaints and annual reports) in a timely manner; responding appropriately and efficiently to questions from stakeholders and the public; responding to data incident reports; and

issuing guidance. The Privacy Office has made substantial progress on many of these priorities, especially increased engagement with the field—particularly entities that provide services and technical assistance to districts, such as boards of cooperative educational services (BOCES) and regional information centers (RICs).

Recent outreach to educational agencies has emphasized that the Department's monitoring for Part 121 compliance will occur in 2023. Indeed, monitoring was identified as a 2023 goal in the Privacy Office's recently issued 2022 Annual Report. Thus, the Department accepts the finding by OSC.[1] Time and additional resources, however, will be critical to support ongoing monitoring.

Monitoring aside, it is important to note that "[n]either the Regents nor the SED is responsible for the day-to-day operation of the schools."[2] "[S]chool districts are independent bodies vested by the State with considerable power."[3] Thus, while the Department anticipates that monitoring will be an effective compliance tool, the obligation to ensure the privacy and security of student data rests with each educational agency.

The Department intends to address Recommendation 1 by:

- Continuing to inform and provide guidance to educational agencies regarding the requirements of Part 121.
- Developing a protocol within the first half of 2023 to monitor educational agencies' compliance with Part 121.
- Begin monitoring educational agencies for compliance with Part 121 within the second half of 2023.

OSC Recommendation 2:

"Continue to work on completing a full data and asset classification of all current Department systems and data."

Department's Response:

We appreciate the auditor's recognition of the Department's prior and ongoing efforts toward completing a full data and asset classification of all current Department systems and data. Although we have made significant progress to identify our systems and data assets, our contractual relationship with NYSTEC will ensure that we develop and establish a formal data classification program efficiently and expeditiously.

OSC's finding and recommendation regarding data and asset classification is, therefore, accepted. We agree that there is more work to be done to improve the classification program and that additional resources will be needed to complete such work.

The Department intends to address Recommendation 2 by:

- Continuing to build upon the partial inventories that have been established.
- Continuing to work with all Department program offices to identify the data assets stored in systems to be properly classified.

---

[1] The Department notes, however, that it periodically contacts all public schools to inform them of their obligation to designate a data privacy officer.
[2] *Campaign for Fiscal Equity, Inc. v. State*, 100 NY2d 893, 904 (2003).
[3] *Paynter v. State*, 270 AD2d 819, 820 (4th Dept 2000).

- Continuing to work with NYSTEC to assist the Department with developing an efficient data classification program.

OSC Recommendation 3:

"Implement the recommendations detailed in the preliminary report to strengthen technical controls over the selected systems reviewed."

Department's Response:

As indicated in its response to the preliminary findings, the Department agrees with all of the audit findings pertaining to technical controls and has begun, and in some cases completed, implementation of the actions the Department stated that it would undertake.

The Department appreciates this opportunity to provide a response to the OSC draft audit report. If you have any additional questions or need additional clarification, please contact Louise DeCandia at Louise.Decandia@nysed.gov.

Yours truly,

Sharon Cates-Williams

c: Commissioner Rosa
Daniel Morton-Bentley
Louise DeCandia
Michael St. John
Marlowe Cochran
James Kampf
Jeanne Day

Contributors to Report

Executive Team

Andrea C. Miller - *Executive Deputy Comptroller*
Tina Kim - *Deputy Comptroller*
Stephen Lynch - *Assistant Comptroller*

Audit Team

Nadine Morrell, CIA, CISM - *Audit Director*
Cynthia Herubin, CIA, CGAP - *Audit Manager*
Daniel Raczynski - *Audit Supervisor*
Justin Dasenbrock, CISA, ITIL - *IT Supervisor*
Christopher Bott - *Examiner-in-Charge*
Nicole Cappiello - *Senior Examiner*
Jonathan Julca - *Senior Examiner*
Kelly Traynor - *Senior Editor*

Contact Information
(518) 474-3271
StateGovernmentAccountability@osc.ny.gov
Office of the New York State Comptroller
Division of State Government Accountability
110 State Street, 11th Floor
Albany, NY 12236

Like us on Facebook at facebook.com/nyscomptroller
Follow us on Twitter @nyscomptroller
For more audits or information, please visit: www.osc.state.ny.us/audits/index.htm