TO: P-12 Education Committee/Higher Education Committee

FROM: Elizabeth R. Berlin

SUBJECT: Proposed Adoption of Part 121 to the Regulations of the Commissioner Relating to Student Data Privacy and Security

DATE: October 3, 2019

AUTHORIZATION(S): Elizabeth R Berlin

SUMMARY

Issue for Discussion

Should the Board of Regents adopt the proposed addition of Part 121 to the Commissioner's regulations to implement Education Law §2-d relating to protecting personally identifiable information?

Reason(s) for Consideration

Required by State statute.

Proposed Handling

The proposed amendment is presented to the P-12 Education Committee for discussion at the October meeting of the Board of Regents. A copy of the proposed rule is included as Attachment A.

Procedural History

At its January 2019 meeting, the Board of Regents was presented with a detailed summary of the proposed amendment and the Board of Regents voted to authorize Department staff to publish the proposed amendment in the State Register for the 60-day public comment period. A Notice of Proposed Rule Making was published in the State Register on January 30, 2019. Following the 60-day public comment period required under the State Administrative Procedure Act, the Department received numerous comments on the proposed amendment. An Assessment of the Public Comment received

during the first public comment period is included as Attachment B. Based on comments received, the Department revised the regulation. A Notice of Revised Rule Making was published in the State Register on July 31, 2019 for a 45-day public comment period. Following the 45-day public comment period required under the State Administrative Procedure Act for revised rule makings, the Department received additional comments on the proposed amendment. An assessment of the public comment received during the second public comment period is included as Attachment C. A Notice of Revised Rule Making will be published in the State Register on October 25, 2019. Supporting materials are available upon request to the Secretary to the Board of Regents.

Background Information

Chapter 56 of the Laws of 2014 added §2-d to the Education Law effective April 2014. The focus of the law is the privacy and security of personally identifiable information (PII) of students, and certain annual professional performance review (APPR) data of teachers and principals. The law outlines certain requirements for educational agencies and their third-party contractors to ensure the security and privacy of such protected information.

Regulatory Background

The proposed amendments to Part 121 of the Commissioner's regulations were developed in consultation with stakeholders and the public. In 2017, the Chief Privacy Officer created the Data Privacy Advisory Council (DPAC) which consists of members drawn from diverse stakeholder groups and includes parents, industry advocates, administrative and teacher organizations and information technology experts. The DPAC created two sub-committees to aid its work: the drafting workgroup and the technical standards workgroup. The drafting workgroup worked on the language of the regulation while the technical standards workgroup (drawn from a cross-section of experts from across the state) was responsible for recommending a standard for educational agency data security and privacy policies and practices. To seek public comments on additional elements of the parent's bill of rights and the regulation, the Department held fourteen public forums across the state in May and June and solicited for electronic comments during this period. The Chief Privacy Officer also created a Regulation Implementation Workgroup comprised of educational agency stakeholders from the field such as RIC Directors, BOCES staff, district technical directors and other experts in the field to collaborate in the work of developing an implementation roadmap, and other tools and resources to aid the adoption and implementation of the regulation and the data security and privacy standard it adopts. The input received from all stakeholders was critical to developing these regulations.

To highlight some provisions, Part 121 clarifies the data privacy and security obligations of educational agencies and third-party contractors; establishes requirements for contracts and other written agreements where PII will be provided to a third-party contractor and also attempts to clarify obligations where click-through agreements for software applications are utilized; establishes the National Institute of Standards and Technology (NIST) Cybersecurity Framework as the standard for educational agencies data security and privacy programs; directs educational agencies to ensure that all

employees that handle PII receive annual data security and privacy training; and requires that educational agencies identify a data protection officer that will be responsible for the educational agency's data privacy and security program.

Proposed Revisions to the Regulation Following the First Public Comment Period

The Department received comments from many diverse groups and individuals including parent and privacy advocates, school district technology directors, school district superintendents, school principals and teachers, BOCES administrators, professional organizations, a professional union, the technology industry and the State Assembly. During preparation of the proposed revised regulations, the Department incorporated suggestions made by the public with respect to the proposed regulation.

At its July Regents meeting, the Department revised the proposed amendments to include the following major changes:

- Provides additional clarity and consistency in the application of certain terms including "Encryption" and "Commercial and Marketing Purpose".
- Provides clarity regarding the complaint process.
- Incorporates sections of the statute where appropriate for completeness.
- Provides educational agencies until July 1, 2020 to adopt and publish a data security and privacy policy.
- Clarifies the requirements of the Data Security and Privacy Plan.
- Clarifies what should be included as part of the annual data privacy and security awareness training.
- Clarifies restrictions on the use or disclosure of personally identifiable information by third party contractors.
- Requires educational agencies to verify that only authorized individuals inspect and review student data.
- Clarifies the authority of the Chief Privacy Officer.

Proposed Revisions to the Regulation Following the Second Public Comment Period

Following the 45-day public comment period required under the State Administrative Procedure Act for revised rule makings, the Department received numerous comments and determined that additional changes are needed to the proposed amendment.

First, based on numerous comments, the Department revised the proposed amendment to remove section 121.9(c) which states that "[w]here a parent or eligible student requests a service or product from a third-party contractor and provides express consent to the use or disclosure of personally identifiable information by the third-party contractor for purposes of providing the requested product or service, such use by the third-party contractor shall not be deemed a marketing or commercial purpose prohibited by this Part."

In addition, the following additional technical amendments were made to the proposed amendment to conform to Education Law §2-d:

- Education Law §2-d (7)(a) provides that the commissioner, in consultation with the chief privacy officer, shall promulgate regulations establishing procedures to implement the provisions of this section, including but not limited to procedures for the submission of complaints from parents and/or persons in parental relation to students, classroom teachers or building principals, or other staff of an educational agency, making allegations of improper disclosure of student data and/or teacher or principal data by a third party contractor or its officers, employees or assignees. The current draft of the proposed amendment only provides a complaint process for parents and eligible students. The proposed amendment has been amended to authorize teachers, principals and staff of the educational agency to utilize the complaint process when there is an improper disclosure of student data and/or teacher or principal data.
- Education Law §2-d(6)(e)(5) states that "if it is determined that the unauthorized release of student data or teacher or principal data on the part of the third party contractor or assignee was inadvertent and done without intent, knowledge, recklessness or gross negligence, the commissioner may determine that no penalty be issued upon the third party contractor." Currently, Section 121.11(f) of the Commissioner's regulations provides that "if the Chief Privacy Officer determines that the breach or unauthorized release of student data or teacher or principal data on the part of the third-party contractor or assignee was inadvertent and done without intent, knowledge, recklessness or gross negligence, the Commissioner may determine that no penalty be issued upon the third-party contractor." There is no reference, however, in either the law or the regulations regarding the process for how the matter gets from the Chief Privacy Officer to the Commissioner. The regulation has been amended to clarify that the Chief Privacy Officer will make a recommendation to the Commissioner for his/her final determination.
- An additional edit was made to the proposed amendment to clarify that the penalty provisions set forth in section 121.11(b) do not apply to the penalties imposed in subdivision (a) of the same section because they are for different types of violations under Education Law §2-d.

Related Regents' Items

- April 2018 Information Privacy Program Update (http://www.regents.nysed.gov/common/regents/files/518p12d1.pdf)

- January 2019 Proposed Addition of Part 121 to the Regulations of the Commissioner Relating to Student Data Privacy (https://www.regents.nysed.gov/common/regents/files/119p12d1.pdf)
- July 2019 Proposed Addition of Part 121 to the Regulations of the Commissioner Relating to Strengthening Data Privacy and Security in NY State Educational Agencies to Protect Personally Identifiable Information (https://www.regents.nysed.gov/common/regents/files/719p12d1-%20REVISED.pdf.)

Recommendation

Not applicable.

Timetable for Implementation

It is anticipated that the proposed amendment will be presented for adoption at the January 2020 Regents meeting, after the publication of the proposed amendment in the State Register and expiration of the 45-day public comment period required under the State Administrative Procedure Act for revised rulemaking. If adopted at the January 2020 meeting, the proposed rule will become effective on January 29, 2020.

ATTACHMENT A

AMENDMENT TO THE REGULATIONS OF THE COMMISSIONER OF EDUCATION

Pursuant to Education Law sections 2-d, 101, 207 and 305,

a new Part 121 shall be added effective upon adoption to read as follows:

Part 121

Strengthening Data Privacy and Security in NY State Educational Agencies to Protect Personally Identifiable Information

§121.1 Definitions.

As used in this Part, the following terms shall have the following meanings:

(a) *Breach* means the unauthorized acquisition, access, use, or disclosure of student data and/or teacher or principal data by or to a person not authorized to acquire, access, use, or receive the student data and/or teacher or principal data.

(b) *Chief Privacy Officer* means the Chief Privacy Officer appointed by the Commissioner pursuant to Education Law §2-d.

(c) *Commercial or Marketing Purpose* means the sale of student data; or its use or disclosure for purposes of receiving remuneration, whether directly or indirectly; the use of student data for advertising purposes, or to develop, improve or market products or services to students.

(d) *Contract or other written agreement* means a binding agreement between an educational agency and a third-party, which shall include but not be limited to an agreement created in electronic form and signed with an electronic or digital signature or a click wrap agreement that is used with software licenses, downloaded and/or online applications and transactions for educational technologies and other technologies in which a user must agree to terms and conditions prior to using the product or service.

(e) *Disclose* or *Disclosure* mean to permit access to, or the release, transfer, or other communication of personally identifiable information by any means, including oral, written, or electronic, whether intended or unintended.

(f) *Education Records* means an education record as defined in the Family Educational Rights and Privacy Act and its implementing regulations, 20 U.S.C. 1232g and 34 C.F.R. Part 99, respectively.

(g) *Educational Agency* means a school district, board of cooperative educational services (BOCES), school, or the Department.

(h) *Eligible Student* means a student who is eighteen years or older.

(i) *Encryption means* methods of rendering personally identifiable information unusable, unreadable, or indecipherable to unauthorized persons through the use of a technology or methodology specified or permitted by the Secretary of the United States department of health and human services in guidance issued under Section 13402(H)(2) of Public Law 111-5.

(j) *FERPA* means the Family Educational Rights and Privacy Act and its implementing regulations, 20 U.S.C. 1232g and 34 C.F.R. Part 99, respectively.

(k) *NIST Cybersecurity Framework* means the U.S. Department of Commerce National Institute for Standards and Technology Framework for Improving Critical Infrastructure Cybersecurity Version 1.1 which is available at the Office of Counsel, State Education Department, State Education Building, Room 148, 89 Washington Avenue, Albany, New York 12234.

(l) *Parent* means a parent, legal guardian, or person in parental relation to a student.

(m) *Personally Identifiable Information*, as applied to student data, means personally identifiable information as defined in section 99.3 of Title 34 of the Code of Federal Regulations implementing the Family Educational Rights and Privacy Act, 20 U.S.C 1232g, and as applied to teacher and principal data, means personally identifiable information as such term is defined in Education Law §3012-c (10).

(n) *Release* shall have the same meaning as Disclosure or Disclose.

(o) *School* means any public elementary or secondary school including a charter school, universal pre-kindergarten program authorized pursuant to Education Law §3602-e, an approved provider of preschool special education, any other publicly funded pre-kindergarten program, a school serving children in a special act school district as defined in Education Law §4001, an approved private school for the education of students with disabilities, a State-supported school subject to the provisions of Article 85 of the Education Law, or a State-operated school subject to the provisions of Articles 87 or 88 of the Education Law .

(p) *Student* means any person attending or seeking to enroll in an educational agency.

(q) *Student Data* means personally identifiable information from the student records of an educational agency.

(r) *Teacher or Principal Data* means personally identifiable information from the records of an educational agency relating to the annual professional performance reviews of classroom teachers or principals that is confidential and not subject to release under the provisions of Education Law §§3012-c and 3012-d.

(s) *Third-Party Contractor* means any person or entity, other than an educational agency, that receives student data or teacher or principal data from an

educational agency pursuant to a contract or other written agreement for purposes of providing services to such educational agency, including but not limited to data management or storage services, conducting studies for or on behalf of such educational agency, or audit or evaluation of publicly funded programs. Such term shall include an educational partnership organization that receives student and/or teacher or principal data from a school district to carry out its responsibilities pursuant to Education Law §211-e and is not an educational agency, and a not-for-profit corporation or other nonprofit organization, other than an educational agency.

(t) *Unauthorized Disclosure or Unauthorized Release* means any disclosure or release not permitted by federal or State statute or regulation, any lawful contract or written agreement, or that does not respond to a lawful order of a court or tribunal or other lawful order.

§121.2 Educational Agency Data Collection Transparency and Restrictions.

(a) Educational agencies shall not sell personally identifiable information nor use or disclose it for any marketing or commercial purpose or facilitate its use or disclosure by any other party for any marketing or commercial purpose or permit another party to do so.

(b) Each educational agency shall take steps to minimize its collection, processing and transmission of personally identifiable information.

(c) Each educational agency shall ensure that it has provisions in its contracts with third party contractors or in separate data sharing and confidentiality agreements that require the confidentiality of shared student data or teacher or principal data be

maintained in accordance with federal and state law and the educational agency's data security and privacy policy.

(d) Except as required by law or in the case of educational enrollment data, school districts shall not report to the department the following student data elements: (1) juvenile delinquency records; (2) criminal records; (3) medical and health records; and (4) student biometric information.

§121.3 Bill of Rights for Data Privacy and Security.

(a) Each educational agency shall publish on its website a parents bill of rights for data privacy and security (“bill of rights”) that complies with the provisions of Education Law §2-d (3).

(b) The bill of rights shall also be included with every contract an educational agency enters with a third-party contractor that receives personally identifiable information.

(c) The bill of rights shall also include supplemental information for each contract the educational agency enters into with a third-party contractor where the third-party contractor receives student data or teacher or principal data. The supplemental information must be developed by the educational agency and include the following information:

(1) the exclusive purposes for which the student data or teacher or principal data will be used by the third-party contractor, as defined in the contract;

(2) how the third-party contractor will ensure that the subcontractors, or other authorized persons or entities to whom the third-party contractor will

disclose the student data or teacher or principal data, if any, will abide by all applicable data protection and security requirements, including but not limited to those outlined in applicable state and federal laws and regulations (e.g., FERPA; Education Law §2-d);

(3) the duration of the contract, including the contract's expiration date and a description of what will happen to the student data or teacher or principal data upon expiration of the contract or other written agreement (e.g., whether, when and in what format it will be returned to the educational agency, and/or whether, when and how the data will be destroyed).

(4) if and how a parent, student, eligible student, teacher or principal may challenge the accuracy of the student data or teacher or principal data that is collected;

(5) where the student data or teacher or principal data will be stored, described in such a manner as to protect data security, and the security protections taken to ensure such data will be protected and data security and privacy risks mitigated; and

(6) address how the data will be protected using encryption while in motion and at rest.

(d) Each educational agency shall publish on its website the supplement to the bill of rights for any contract or other written agreement with a third-party contractor that will receive personally identifiable information.

(e) The bill of rights and supplemental information may be redacted to the extent necessary to safeguard the privacy and/or security of the educational agency's data and/or technology infrastructure.

§121.4 Complaints of Breach or Unauthorized Release of Personally Identifiable Information

(a) Each educational agency must establish and communicate to parents, eligible students, teachers, principals or other staff of an educational agency, its procedures for them to file complaints about breaches or unauthorized releases of student data and/or teacher or principal data.

(b) The complaint procedures must require educational agencies to promptly acknowledge receipt of complaints, commence an investigation, and take the necessary precautions to protect personally identifiable information.

(c) Following its investigation of a submitted complaint, the educational agency shall provide the parent or eligible student, teacher, principal or any other staff member of the educational agency who filed a complaint with its findings within a reasonable period but no more than 60 calendar days from the receipt of the complaint by the educational agency. Where the educational agency requires additional time, or where the response may compromise security or impede a law enforcement investigation, the educational agency shall provide the parent, eligible student, teacher, principal or any other staff member of the educational agency who filed a complaint with a written explanation that includes the approximate date when the educational agency anticipates that it will respond to the complaint.

(d) Educational agencies may require complaints to be submitted in writing.

(e) Educational agencies must maintain a record of all complaints of breaches or unauthorized releases of student data and their disposition in accordance with

applicable data retention policies, including the Records Retention and Disposition Schedule ED-1 (1988; rev. 2004), as set forth in section 185.12, Appendix I of this Title.

§121.5 Data Security and Privacy Standard.

(a) As required by Education Law §2-d (5), the Department adopts the National Institute for Standards and Technology Framework for Improving Critical Infrastructure Cybersecurity Version 1.1 (NIST Cybersecurity Framework or NIST CSF) as the standard for data security and privacy for educational agencies.

(b) No later than July 1, 2020, each educational agency shall adopt and publish a data security and privacy policy that implements the requirements of this Part and aligns with the NIST CSF.

(c) Each educational agency's data security and privacy policy must also address the data privacy protections set forth in Education Law §2-d (5)(b)(1) and (2) as follows:

(1) every use and disclosure of personally identifiable information by the educational agency shall benefit students and the educational agency (e.g., improve academic achievement, empower parents and students with information, and/or advance efficient and effective school operations).

(2) personally identifiable information shall not be included in public reports or other documents.

(d) An educational agency's data security and privacy policy shall include all the protections afforded to parents or eligible students, where applicable, under FERPA

and the Individuals with Disabilities Education Act (20 U.S.C. 1400 et seq.), and the federal regulations implementing such statutes.

(e) Each educational agency must publish its data security and privacy policy on its website and provide notice of the policy to all its officers and employees.

§121.6 Data Security and Privacy Plan.

(a) Each educational agency that enters into a contract with a third-party contractor shall ensure that the contract includes the third-party contractor's data security and privacy plan that is accepted by the educational agency. The data security and privacy plan shall, at a minimum:

(1) outline how the third-party contractor will implement all state, federal, and local data security and privacy contract requirements over the life of the contract, consistent with the educational agency's data security and privacy policy;

(2) specify the administrative, operational and technical safeguards and practices it has in place to protect personally identifiable information that it will receive under the contract;

(3) demonstrate that it complies with the requirements of Section 121.3(c) of this Part;

(4) specify how officers or employees of the third-party contractor and its assignees who have access to student data, or teacher or principal data

receive or will receive training on the federal and state laws governing confidentiality of such data prior to receiving access;

(5) specify if the third-party contractor will utilize sub-contractors and how it will manage those relationships and contracts to ensure personally identifiable information is protected;

(6) specify how the third-party contractor will manage data security and privacy incidents that implicate personally identifiable information including specifying any plans to identify breaches and unauthorized disclosures, and to promptly notify the educational agency;

(7) describe whether, how and when data will be returned to the educational agency, transitioned to a successor contractor, at the educational agency's option and direction, deleted or destroyed by the third-party contractor when the contract is terminated or expires.

§121.7 Training for Educational Agency Employees.

Educational agencies shall annually provide data privacy and security awareness training to their officers and employees with access to personally identifiable information. Such training should include but not be limited to training on the state and federal laws that protect personally identifiable information, and how employees can comply with such laws. Such training may be delivered using online training tools and may be included as part of training the educational agency already offers to its workforce.

§121.8 Educational Agency Data Protection Officer

(a) Each educational agency shall designate a Data Protection Officer to be responsible for the implementation of the policies and procedures required in Education Law §2-d and this Part, and to serve as the point of contact for data security and privacy for the educational agency.

(b) Data Protection Officers must have the appropriate knowledge, training and experience to administer the functions described in this Part.

(c) A current employee of an educational agency may perform this function in addition to other job responsibilities.

§121.9 Third Party Contractors

(a) In addition to all other requirements for third-party contractors set forth in this Part, each third-party contractor that will receive student data or teacher or principal data shall:

(1) adopt technologies, safeguards and practices that align with the NIST Cybersecurity Framework;

(2) comply with the data security and privacy policy of the educational agency with whom it contracts; Education Law § 2-d; and this Part;

(3) limit internal access to personally identifiable information to only those employees or sub-contractors that need access to provide the contracted services;

(4) not use the personally identifiable information for any purpose not explicitly authorized in its contract;

(5) not disclose any personally identifiable information to any other party without the prior written consent of the parent or eligible student:

(i) except for authorized representatives of the third-party contractor such as a subcontractor or assignee to the extent they are carrying out the contract and in compliance with state and federal law, regulations and its contract with the educational agency; or

(ii) unless required by statute or court order and the third-party contractor provides a notice of disclosure to the department, district board of education, or institution that provided the information no later than the time the information is disclosed, unless providing notice of disclosure is expressly prohibited by the statute or court order.

(6) maintain reasonable administrative, technical and physical safeguards to protect the security, confidentiality and integrity of personally identifiable information in its custody;

(7) use encryption to protect personally identifiable information in its custody while in motion or at rest; and

(8) not sell personally identifiable information nor use or disclose it for any marketing or commercial purpose or facilitate its use or disclosure by any other party for any marketing or commercial purpose or permit another party to do so.

(b) Where a third-party contractor engages a subcontractor to perform its contractual obligations, the data protection obligations imposed on the third-party contractor by state and federal law and contract shall apply to the subcontractor.

§121.10 Reports and Notifications of Breach and Unauthorized Release

(a) Third-party contractors shall promptly notify each educational agency with which it has a contract of any breach or unauthorized release of personally identifiable information in the most expedient way possible and without unreasonable delay but no more than seven calendar days after the discovery of such breach.

(b) Each educational agency shall in turn notify the Chief Privacy Officer of the breach or unauthorized release no more than 10 calendar days after it receives the third-party contractor's notification using a form or format prescribed by the Department.

(c) Third-party contractors must cooperate with educational agencies and law enforcement to protect the integrity of investigations into the breach or unauthorized release of personally identifiable information.

(d) Educational agencies shall report every discovery or report of a breach or unauthorized release of student, teacher or principal data to the Chief Privacy Officer without unreasonable delay, but no more than 10 calendar days after such discovery.

(e) Educational agencies shall notify affected parents, eligible students, teachers and/or principals in the most expedient way possible and without unreasonable delay, but no more than 60 calendar days after the discovery of a breach or unauthorized release by an educational agency or the receipt of a notification of a breach or unauthorized release from a third-party contractor unless that notification would interfere with an ongoing investigation by law enforcement or cause further disclosure of personally identifiable information by disclosing an unfixed security vulnerability. Where notification is delayed under these circumstances, the educational agency shall notify parents, eligible students, teachers and/or principals within seven

calendar days after the security vulnerability has been remedied or the risk of interference with the law enforcement investigation ends.

(f) Where a breach or unauthorized release is attributed to a third-party contractor, the third-party contractor shall pay for or promptly reimburse the educational agency for the full cost of such notification.

(g) Notifications required by this section shall be clear, concise, use language that is plain and easy to understand, and to the extent available, include: a brief description of the breach or unauthorized release, the dates of the incident and the date of discovery, if known; a description of the types of personally identifiable information affected; an estimate of the number of records affected; a brief description of the educational agency's investigation or plan to investigate; and contact information for representatives who can assist parents or eligible students that have additional questions.

(h) Notification must be directly provided to the affected parent, eligible student, teacher or principal by first-class mail to their last known address; by email; or by telephone.

(i) Upon the belief that a breach or unauthorized release constitutes criminal conduct, the Chief Privacy Officer shall report such breach and unauthorized release to law enforcement in the most expedient way possible and without unreasonable delay.

§121.11 Third Party Contractor Civil Penalties

(a) Each third party contractor that receives student data or teacher or principal data pursuant to a contract or other written agreement with an educational

agency shall be required to notify such educational agency of any breach of security resulting in an unauthorized release of such data by the third party contractor or its assignees in violation of applicable state or federal law, the parents bill of rights for student data privacy and security, the data privacy and security policies of the educational agency and/or binding contractual obligations relating to data privacy and security, in the most expedient way possible and without unreasonable delay. Each violation of this paragraph by a third-party contractor shall be punishable by a civil penalty of the greater of $5,000 or up to $10 per student, teacher, and principal whose data was released, provided that the latter amount shall not exceed the maximum penalty imposed under General Business Law §899-aa (6) (a).

(b) Except as otherwise provided in subdivision (a) each violation of Education Law §2-d by a third-party contractor or its assignee shall be punishable by a civil penalty of up to $1,000.00; a second violation by the same third party contractor involving the same data shall be punishable by a civil penalty of up to $5,000; any subsequent violation by the same third party contractor involving the same data shall be punishable by a civil penalty of up to $10,000. Each violation shall be considered a separate violation for purposes of civil penalties and the total penalty shall not exceed the maximum penalty imposed under General Business Law §899-aa (6) (a).

(c) The Chief Privacy Officer shall investigate reports of breaches or unauthorized releases of student data or teacher or principal data by third-party contractors. As part of an investigation, the Chief Privacy Officer may require that the parties submit documentation, provide testimony, and may visit, examine and/or inspect the third-party contractor's facilities and records.

(d) Upon conclusion of an investigation, if the Chief Privacy Officer determines that a third-party contractor has through its actions or omissions caused student data or teacher or principal data to be breached or released to any person or entity not authorized by law to receive such data in violation of applicable state or federal law, the data and security policies of the educational agency, and/or any binding contractual obligations, the Chief Privacy Officer shall notify the third-party contractor of such finding and give the third-party contractor no more than 30 days to submit a written response.

(e) () If after reviewing the third-party contractor's written response, the Chief Privacy Officer determines the incident to be a violation of Education Law §2-d, the Chief Privacy Officer shall be authorized to:

(1) order the third-party contractor be precluded from accessing personally identifiable information from the affected educational agency for a fixed period of up to five years; and/or

(2) order that a third-party contractor or assignee who knowingly or recklessly allowed for the breach or unauthorized release of student data or teacher or principal data be precluded from accessing student data or teacher or principal data from any educational agency in the state for a fixed period of up to five years; and/or

(3) order that a third party contractor who knowingly or recklessly allowed for the breach or unauthorized release of student data or teacher or principal data shall not be deemed a responsible bidder or offeror on any contract with an educational agency that involves the sharing of student data or teacher or principal data, as applicable for purposes of the provisions of

General Municipal Law §103 or State Finance Law §163(10)(c), as applicable, for a fixed period of up to five years;

(4) require the third-party contractor to provide additional training governing confidentiality of student data and/or teacher or principal data to all its officers and employees with reasonable access to such data and certify that it has been performed, at the contractor's expense. Such additional training must be performed immediately and include a review of federal and state laws, rules, regulations, including Education Law §2-d and this Part.

(f) If the Chief Privacy Officer determines that the breach or unauthorized release of student data or teacher or principal data on the part of the third-party contractor or assignee was inadvertent and done without intent, knowledge, recklessness or gross negligence, the Chief Privacy Officer would make a recommendation to the Commissioner that no penalty be issued upon the third-party contractor. The Commissioner would then make a final determination as to whether the breach or unauthorized release of student data or teacher or principal data on the part of the third-party contractor or assignee was inadvertent and done without intent, knowledge, recklessness or gross negligence and whether or not a penalty should be issued.

§121.12 Right of Parents and Eligible Students to Inspect and Review Students Education Records

(a) Consistent with the obligations of the educational agency under FERPA, parents and eligible students shall have the right to inspect and review a student's education record by making a request directly to the educational agency in a manner prescribed by the educational agency.

(b) An educational agency shall ensure that only authorized individuals are able to inspect and review student data. To that end, educational agencies shall take steps to verify the identity of parents or eligible students who submit requests to inspect and review an education record and verify the individual's authority to do so.

(c) Requests by a parent or eligible student for access to a student's education records must be directed to an educational agency and not to a third-party contractor. An educational agency may require that requests to inspect and review education records be made in writing.

(d) Educational agencies are required to notify parents annually of their right to request to inspect and review their child's education record including any student data stored or maintained by an educational agency. A notice issued by an educational agency to comply with the FERPA annual notice requirement shall be deemed to satisfy this requirement. Two separate annual notices shall not be required.

(e) Educational agencies shall comply with a request for access to records within a reasonable period, but not more than 45 calendar days after receipt of a request.

(f) Educational agencies may provide the records to a parent or eligible student electronically, if the parent consents to such a delivery method. The educational agency must transmit the personally identifiable information in a way that complies with State and federal law and regulations. Safeguards associated with industry standards

and best practices, including but not limited to, encryption and password protection, must be in place when education records requested by a parent or eligible student are electronically transmitted.

§121.13 Chief Privacy Officer's Powers

(a) The Chief Privacy Officer shall have the power to access all records, reports, audits, reviews, documents, papers, recommendations, and other materials maintained by an educational agency that relate to student data or teacher or principal data, which shall include but not be limited to records related to any technology product or service that will be utilized to store and/or process personally identifiable information.

(b) Based upon a review of such records, the Chief Privacy Officer may require an educational agency to act to ensure that personally identifiable information is protected in accordance with state and federal law and regulations, including but not limited to requiring an educational agency to perform a privacy impact and security risk assessment.

(c) The Chief Privacy Officer shall also have and exercise any other powers that the commissioner shall deem appropriate.

§ 121.14 Severability.

If any provision of this Part or its application to any person or circumstances is adjudged invalid by a court of competent jurisdiction, such judgment shall not affect or impair the validity of the other provisions of this Part or their application to other persons

and circumstances, and those remaining provisions shall not be affected but shall remain in full force and effect.

ATTACHMENT B

ASSESSMENT OF PUBLIC COMMENT

Following publication of the Notice of Revised Rule Making in the State Register on July 31, 2019, the Department received the following comments on the proposed amendment:

1. COMMENT: Many commenters wrote to urge the Department not to weaken the provisions of Education Law §2-d by permitting college testing companies to sell or commercialize student data. Several commenters wrote to "oppose the radically weakening of the student privacy law, Education Law §2-d." They stated that "these proposed regulations would encourage the further commercialization and marketing of personal student data". Another commenter 'vehemently' opposed the sale of student data and stated that "sale of their information to outside parties is a violation of their privacy and may be used to discriminate against them in future endeavors."

   RESPONSE: The rule as written is consistent with Education Law §2-d and section 121.9(a)(8) prohibits any third party contractor from selling any personally identifiable information or using or disclosing it for any marketing or commercial purpose or facilitating its use or disclosure by any other party for any marketing or commercial purpose or permitting another party to do so.

2. COMMENT: A commenter asked the Department to focus on “strengthening the Parent Bill of Rights and rigorously enforcing the law, to ensure that the widespread collection and disclosure of my child’s sensitive data is minimized and kept safe from breach and abuse.”

   RESPONSE: No change is necessary. The Department believes the provisions of the proposed amendment relating to the Parent Bill of Rights complies with Education Law §2d. Therefore, no change is warranted.

3. COMMENT: A commenter stated that the Department should state that “not all of the NIST CSF standards will be applicable to districts as they do not apply to K-12 education and would be problematic. The same commenter requested a staggered adoption timeline; and asked in situations where a BOCES is the sole party to a contract with a third-party contractor, the proposed regulation allow for an exception to the requirement for direct notification from the educational agency to the affected students/parents and teachers and principals because BOCES does not possess the personally identifiable information that would be required in order to provide such notice. The commenter suggests to instead require that the BOCES, using information it obtains from the third party contractor, to assist the school districts by preparing a draft of the required notice and providing it to affected districts. Each school district would then make a determination, in consultation with the BOCES, whether under the particular circumstances the notice will be signed by the district, the BOCES, or both.

   The same commenter stated that the regulatory impact statement (RIS) filed by the Department is insufficient.

RESPONSE: No change is necessary. The NIST Cybersecurity Framework is recognized nationally and used internationally as a flexible, cost-effective and risk-based standard that helps entities protect their critical or sensitive infrastructure. The NIST Standards do not apply to one specific sector and therefore the Department believes the standards are applicable to school settings. If a control in the Framework is not applicable to an educational agency, there is no requirement for it to apply. Educational agencies will use the standards to address their vulnerability to cybersecurity and data privacy threats so that they can address those identified vulnerabilities using a prioritized approach. Further, because each agency's risk-based prioritization will be unique, implementation will be inherently staggered. Regarding the notification requirement where a BOCES is the sole contractor with a third-party contractor, the Department has considered the comment but has determined no change is necessary. Regarding the RIS, the Department revised its original Regulatory Impact Statement as part of the Notice of Revised Rule Making published on July 31, 2019 to help clarify that since the NIST standard is not a one size fits all standard and it has not been implemented in New York State prior to this time, the Department does not have data that would enable it to quantify an expected cost.

4. COMMENT: A Commenter wrote: "how about focusing on... safety in schools. more illegal drug education. counseling in general for mental health so our kids of tomorrow can be safe in running our country when we are old. strategies so that special needs kids have the proper education and the same possibilities as

general ed students classes on general life skills bring back home economics. make our kids better not just a profit!”

RESPONSE: No change is necessary as this comment is beyond the scope of the regulation.

5. COMMENT: A Commenter asked the Department to “Please protect student privacy!”

   RESPONSE: No change is necessary. The purpose of the statute and the proposed rule is to strengthen the data privacy and security posture and practices of educational agencies and protect the privacy and security of student data.

6. COMMENT: The Department received letters from commenters who were concerned that the regulation would impede the access of colleges and universities to student data that enables these organizations from sending targeted mailings to high school seniors. Some institutions stated that the regulation appeared to require parental consent for the College Board to release information to colleges and universities contrary to historical practice. Some of these organizations stated that requiring consent would have “a chilling impact on first-generation and underrepresented college student enrollment as well as adversely impact all students on their journey towards making a college choice that is right for them individually and as a family.” The commenters expressed “very grave concerns that the proposed regulations would place additional barriers and unintended consequences to entry on high school students

attempting to take the next step to college" and explained that "currently, all students taking college entrance exams (SAT, ACT, PSAT) can opt in to have their information, including their scores, sent to colleges and universities, thereby allowing the institutions to send those students informational material that help them understand their college options."

Along similar lines, another commenter stated that the ability for students to opt in for a chance to have colleges and universities send them informational materials "has proven to increase the chances a student applies and enrolls at a college, especially for underrepresented populations such as first-generation college students" because in some cases, this outreach by universities may be the primary source of information about college opportunities. These commenters stated that the proposed regulation "would have an unintended consequence of limiting students taking the college entrance exams – most of whom are under 18 years old – ability to receive critical informational materials from colleges and universities" and that requiring parental consent "simply adds another barrier, especially for underrepresented populations who may live in non-parental homes, to learn about institutions that may be a good fit for their higher education pursuits."

Yet another commenter asked the Department to revise the proposed rule to preserve the "current requirement for student consent for information to be shared" or alternatively, separate the issue from the rest of the regulatory package to avoid harming educational opportunities for students who are low income and students of color.

Another commenter asked the Department to clarify that students under 18 would be allowed to consent to the disclosure of their personally identifiable information to colleges and universities.

RESPONSE: The Department is committed to promoting sound information practices and policies that will ensure the security and privacy of student data and improve academic achievement. The Department has removed section 121.9(c) of the proposed regulation. To the extent the commenter seeks a response on a specific set of circumstances and activities of the College Board, it would depend on the facts and circumstances of each disclosure of any student data or teacher or principal data as to how Education Law §2-d would apply. The proposed amendment merely implements the law.

7. COMMENT: A commenter asked the Department not to "give in to yet another effort to turn education and information over to private corporations. Public education should be by, for, and about the public, not corporations."

   RESPONSE: No change is necessary. The purpose of the proposed rule is to strengthen the data privacy and security posture and practices of educational agencies.

8. COMMENT: Another commenter stated that "it's only fair to have all teachers and other school personnel including the superintendent to have the same privacy as students. Give or sell it and include all persons in the school."

   RESPONSE: No change is necessary. This comment is outside the scope of the proposed regulation.

9. COMMENT: A commenter stated regarding her daughter that “it is both ironic and frightening that legislation is being considered that will allow companies and vendors to invade her digital privacy without first obtaining her consent or the consent of her parents. Clearly the desires of wealthy corporations are being prioritized over the rights of our children.”

   RESPONSE: Education Law §2-d(5)(f) and section 121.9(a)(4) of the proposed amendment require that each third party contractor that enters into a contract or other written agreement with an educational agency under which the third party contractor will receive student data or teacher or principal data not disclose any personally identifiable information to any other party without the prior written consent of the parent or eligible student. .

10. COMMENT: A commenter stated that the proposed changes “should have been flagged and memoed to all schools and been the subject of discussions at PTA meetings not debated in settings and times obscure to the affected public school families.” The commenter further stated that they believed the number of public forums held in 2018 to be inadequate.

    RESPONSE: No change is necessary. In addition to the 14 public forums held across the state, the proposed rule has undergone two public comment periods, for 60 and 45 days respectively. Further, the executive Director of the NYS Parent Teachers Association served on the Department’s Data Privacy Advisory Council along with other stakeholders.

11. COMMENT: A commenter stated that “the people who want to make a buck at the expense of our children have been degrading education since No Child Left Behind. Do YOU want to continue the Bush legacy? Please be a hero for the students. They only get one chance at a public education.” Another commenter stated that “Our children cannot give consent to their personal information being shared for commercial purposes, yet they will never be able to take the information back if it is shared by the adults who should be protecting them.”
RESPONSE: The proposed regulation is consistent with the provisions of Education Law §2-d. See also responses to Comments #1 and #9. Therefore, no change is necessary.

12. COMMENT: A commenter stated that Education Law Section 2-d is designed to deal with relationships between educational institutions and third-party contractors and opined that college admissions testing companies such as College Board are not third-party contractors under this law.
RESPONSE: No change is necessary. See Response to #6.

13. COMMENT: A commenter asked that an exception be made to permit third party contractors to use personally identifiable information to provide services contracted by a district if it is for a limited purpose and is in compliance with all applicable laws and regulations.
RESPONSE: No change is required. The requirements relating to third-party contractors in the proposed amendment is consistent with the requirements set forth in Education Law §2-d.

14. COMMENT: A commenter expressed concern that the provision outlined in §121.11 of the proposed rule that states that “the Chief Privacy Officer may visit, examine and/or inspect a third party contractor’s facilities and records in the event of a breach or unauthorized release of student or teacher data” may be in conflict with the third party contractor’s similar privacy obligations to other customers.

RESPONSE: The proposed rule as written is consistent with the provisions of the Education Law §2-d. No change is necessary.

15. COMMENT: A commenter stated that Section 121.1. Definition of "Commercial or Marketing Purpose" of the proposed regulation expands the scope of Education Law § 2-d and may be interpreted in a manner that may restrict beneficial programs or create technical compliance concerns. The commenter stated that the definition fails to distinguish between various types of activities such as the sale of student data to a third party for commercial gain, informing students about beneficial programs (such as scholarship programs), and internal use of data to improve the provider's own service.

RESPONSE: The Department believes the referenced provision is consistent with the intent of the underlying statute. Therefore, no change is necessary.

16. COMMENT: A commenter stated that the proposed regulation does not distinguish between the use of "directory information" (as defined in FERPA) and more sensitive educational records, which may result in the regulation requiring

parent consent for programs that only use a small amount of less-sensitive directory data.

RESPONSE: The proposed rule, has been revised to remove the parental consent requirement under section 121.9(c), therefore no change is necessary.

17. COMMENT: With regards to Section 121.1's definition of "Commercial or Marketing Purpose," a commenter stated that the inclusion of the phrase "directly or indirectly," coupled with the reference to sale, use, disclosure and marketing in the same provision, creates interpretive questions and potential ambiguity. The comment stated that it may be hard for a service provider to discern if a use or disclosure is permitted, or if it puts the service provider at risk of allegedly using or disclosing information "indirectly" for purposes of receiving remuneration. The same commenter stated that the use of "advertising" in the same section should be explicitly limited to advertising for commercial products and services, as is the case in similar statutes addressing the same underlying commercialization concern. The commenter further stated that the clause "develop, improve or market products or services" should distinguish between internal use on the one hand, and disclosure to third parties for commercial purposes on the other, and should be modified to apply to commercial products and services.

RESPONSE: The proposed rule, as written, is consistent with Education Law §2-d which prohibits the sale or use of personally identifiable information for marketing or commercial purposes, and does not make the distinction described above. The statute also prohibits the use of personally identifiable information for any purposes not explicitly authorized in the contract. No change is necessary.

18. COMMENT: A commenter stated that educational agencies should retain flexibility to approve contracts that include communications with students about beneficial educational programs such as scholarships, college access, enrichment and similar programs without requiring parent consent for school-endorsed programs so that students are not deprived of access to lawful and beneficial services.

RESPONSE: While the Department agrees that an educational agency should communicate with students about beneficial educational programs such as scholarships, college access, enrichment and similar programs, it must determine whether each disclosure fits within the ambits of Education Law §2-d depending on the facts and circumstances. Moreover, to the extent the comment is challenging the parental consent requirement under section 121.9(c), that provision has been removed. See also Response #9.

19. COMMENT: A commenter expressed concern that the requirement to post supplemental information on the educational agency's website contained in section 121.3. may expose information to hackers that could put student data at risk and stated that redaction should be permitted at the request of the contractor or based on a joint determination between the contractor and the agency and that this determination should not be made by the agency alone.

RESPONSE: This is addressed in the proposed rule as it provides that the bill of rights and supplemental information may be redacted to the extent necessary to

safeguard the privacy and/or security of the educational agency's data and/or technology infrastructure. No change is necessary.

20. COMMENT: A commenter stated that the clause in Section 121.6 of the proposed rule that refers to data being deleted, destroyed or transferred back to the educational agency at the end of the contract should also permit the transfer of student-generated content or similar data to a personal account at the request of the student or parent to enable families retain content or data in online accounts.

RESPONSE: The proposed amendment was intended to ensure that data is deleted, destroyed or transferred back at the end of the contract period. The regulation does not prohibit educational agencies from negotiating such clauses with their third-party contractors subject to applicable provisions of state and federal law and regulation.

21. COMMENT: A commenter wrote that the provision in Section 121.9 prohibiting disclosure of personally identifiable information to any third party without the written consent of the parent or eligible student should refer to "consent of the educational agency, the parent or eligible student or the affected teacher or principal, as applicable" and should permit the educational agency to consent to disclosures which are part of a school approved service or program. The commenter stated that without clarification, clauses (5) and (8) may conflict with

clause (a)(4) and require parent consent for educational programs that are otherwise permitted under FERPA and undertaken with the consent of the agency.

RESPONSE The Department has revised the proposed regulation to remove Section 121.9(c). Therefore, no change is necessary. See also Response to #9.

22. COMMENT: A commenter suggested more time for educational agencies and third-party contractors to comply with the proposed rule.

RESPONSE: Education Law §2-d became effective on March 31, 2014 and the proposed amendment implements the statutory provisions and was published in the State Register on January 30, 2019 and it is anticipated that the proposed amendment will be adopted at the January 2020 meeting. Therefore, the Department does not believe any change to the proposed regulation to add a timeline or additional time is needed.

23. COMMENT: A commenter stated that the Department should ‘push away from the focus as standardized, computer based testing as the end all/be all of tracking student progress/achievement” and “stop trying to sell parents on the importance of state testing.” The commenter also stated that “we need to move towards need based school funding” and provide training in soft skills to students.

RESPONSE: Since the comment is outside the scope of the regulation, no response is necessary.

24. COMMENT: A commenter stated that they were pleased that the revised regulation “includes an exception for promotion of colleges, scholarships, tutoring services, educational materials and related resources with prior consent of a parent or legal guardian.”

    RESPONSE: There is no specific exception in the proposed regulations for the promotion of colleges, scholarships, tutoring services, educational materials and related resources. See also Response #18.

25. COMMENT: A commenter wrote “to share my extreme discontent over the New York State Board of Education’s consideration of the sharing of student data for marketing purposes. Please keep in mind the strong thoughts on this matter from parents like myself who are extremely concerned about how many hands are in the pot when it comes to the education of our children. We need teachers to be in the forefront of advising parents on educational decisions and not big business looking to make a profit and confusing us with their sales pitches. I implore you to please respect the data privacy of our students! Make New York a model of what is right in education and not a billboard for the use of outside vendors!”

    RESPONSE: Please see response to Comment #1.

26. COMMENT: A commenter opined that the definition of “commercial or marketing purpose” goes beyond the scope and intention of the law and could cause some unintended consequences. They stated that the current draft language “stifles innovation by limiting the ability of EdTech providers to be able to offer improved products and services based on student use of the product” and that the phrases

" 'develop or improve' effectively negates the very purpose and promise of technology in the classroom – that students would have access to the most up to date tools and content for learning." The commenter stated that "without data to improve and develop new technology, schools would never find useful products or easy to use products as they'd just be developed in a vacuum of any real world application."

RESPONSE: The Department believes the definition of commercial or marketing purpose is consistent with the intent of Education Law §2-d which is to ensure the privacy and the security of student and teacher data. See also Response to #9.

27. COMMENT: Another comment stated that the phrase the "use or disclosure for purposes of receiving remuneration, whether directly or indirectly" could prohibit schools from contracting for services with any outside organization because businesses making education technology products, by the nature of being a business, profit from the sales of their products, and requested that the language be stricken from the regulations.

RESPONSE: The Department believes this definition is consistent with the intent of Education Law §2-d. Therefore, no change is necessary. Also see response to #9.

28. COMMENT: A commenter agreed that subcontractors should be required to protect data according to the contract signed by the third party provider and proposed language they believed would strengthen the proposed rule. The

commenter, while recognizing that their suggestion was a repeat of their comment during the first round of comments, suggested that the Department revise the proposed rule to require: “an assurance that the third party contractor will (a) prohibit the subcontractor from using student data or teacher or principal data for any purpose other than providing the contracted service to, or on behalf of, the third party contractor, (b) prohibits the subcontractor from disclosing student data or teacher or principal data provided by the third party contractor to subsequent third parties, and (c) requires the subcontractor to comply with subsection 1.1 of this section.”.

RESPONSE: The proposed rule provides that where a third-party contractor engages a subcontractor to perform its contractual obligations, the data protection obligations imposed on the third-party contractor by state and federal law and contract shall apply to the subcontractor. Therefore, the Department does not believe an amendment is necessary.

29. COMMENT: A comment stated that the inclusion of third party providers in the regulatory development process would “have provided other stakeholders and regulators with crucial field information on current use and practice as well as greatly reduce the chance of unintended consequences with the result being robust, balanced protections for students.” The commenter stated that the Future of Privacy Forum is not an advocate for industry but a group that brings all stakeholders together and requested that industry participation should be sought in the future.

RESPONSE: The proposed amendments to Part 121 of the Commissioner's regulations were developed in consultation with stakeholders and the public. In 2017, the Chief Privacy Officer created the Data Privacy Advisory Council (DPAC) which consists of members drawn from diverse stakeholder groups and includes parents, industry advocates, administrative and teacher organizations and information technology experts. The DPAC created two sub-committees to aid its work: the drafting workgroup and the technical standards workgroup. The drafting workgroup worked on the language of the regulation while the technical standards workgroup (drawn from a cross-section of experts from across the state) was responsible for recommending a standard for educational agency data security and privacy policies and practices. To seek public comments on additional elements of the parent's bill of rights and the regulation, the Department held fourteen public forums across the state in May and June and solicited for electronic comments during this period. The Chief Privacy Officer also created a Regulation Implementation Workgroup comprised of educational agency stakeholders from the field such as RIC Directors, BOCES staff, district technical directors and other experts in the field to collaborate in the work of developing an implementation roadmap, and other tools and resources to aid the adoption and implementation of the regulation and the data security and privacy standard it adopts. The input received from all stakeholders was critical to developing these regulations.

The Department recognizes the value having a diverse group of stakeholders involved in the regulatory development process and will take this comment into consideration for the future. However, the regulation was developed after 14

public forums were held across the state and he proposed rule has undergone two public comment periods, for 60 and 45 days respectively. Further, the executive Director of the NYS Parent Teachers Association served on the Department's Data Privacy Advisory Council along with other stakeholders.

30. COMMENT: A commenter noted that requests for information and vendor contracts can include multiple districts, and questioned whether posting a vendor signed copy of the Bill of Rights from a contract that includes multiple districts would fulfill the supplemental requirement for each individual district, since there will not be individual copies of the Bill of Rights for each district when multiple districts are included in the contract.

RESPONSE: The Department will issue guidance to aid educational agencies in their implementation of the proposed rule. The purpose of §121.3 (c) of the proposed amendment is to promote transparency and accountability when it comes to the use of and granting of access to personally identifiable information (PII). Where multiple districts utilize a consortium contract or piggy back off another district's contract with a third-party contractor, such an educational agency may utilize the supplemental information from that contract as long as it complies with the requirements of the statute and the proposed rule, and the supplemental information is accurate rule as it applies to the educational agency. For instance, supplemental information about the duration of the contract and the exclusive purpose for which the PII will be utilized must be accurate. No change is necessary.

31. COMMENT: A commenter questioned whether other vendors/agencies should be able to distribute materials related to Education Law §2-d without oversight and approval from the Department's privacy division.
RESPONSE: The Chief Privacy Officer will assist and provide guidance to the field on issues related to Education Law §2-d..

32. COMMENT: A commenter suggested a revision which specifies that the protections of Education Law §2-d apply to any contractual relationship established prior to the proposed rule's effective date. Another commenter stated that the proposed rule would permit educational agencies to structure contractual arrangements to avoid compliance with Education Law §2-d and recommended it be revised to provide that NYSED will audit contracts to ensure they are structured appropriately to comply with the student data privacy protections set forth in Education Law §2-d and the proposed rule.
RESPONSE: The proposed rule implements Education Law §2-d. Regardless of the effective date of the rule, the relevant provisions of Education Law §2-d have been in effect and applicable to educational agency contracts since March 31, 2014. These obligations extend to sub-contractors as well. The Department does not believe that the requirements of the statute and the proposed rule can be avoided through contractual arrangements. Therefore, no change is needed.

33. COMMENT: A commenter requests that the definition of "third-party contractor" should be revised to include not only entities that "receive" student, teacher or principal data, but entities that also "have access to" student, teacher,

and parent data, including those that “collect”, “process”, “disclose”, “use” or “monetize” this data because vendors that host a server or provide software may claim they do not actively “receive” student data and would therefore not need to comply with Education Law §2-d or the proposed regulation. The commenter also notes that while the proposed regulation provides penalties in the case of a breach of PII by a third party contractor, they do not contain penalties that would apply to a school district for breach of PII and suggest that the proposed regulation should be amended to include such.

RESPONSE: No change is necessary. The language of the proposed rule mirrors Education Law §2-d.

34. COMMENT: A commenter raised the issue of educational agency compliance when utilizing systems pursuant to a click-wrap agreement and expressed concern that educational agencies may “not be able to use these systems at all, or there could be a great deal of work involved in compliance.” The commenter also states that complexity of the task of compliance with the supplemental information to be included in the Parent Bill of Rights depends on the final determination on the use of products utilizing click-wrap agreements. The commenter requested additional discussions be held on this issue.

RESPONSE: No change is necessary. The requirements of the statute apply regardless of the form of contract utilized and making an exception from compliance merely based on the form of contracting would not align with the purpose of the statute to protect personally identifiable information. The Department acknowledges the issues raised regarding such agreements, and will provide

guidance, as needed, to assist educational agencies in meeting the requirements of the proposed rule.

35. COMMENT: A commenter stated that “instituting a DPO by December 2019 will present significant implementation challenges.” The commenter highlighted the fact that the DPO would need to have a unique set of qualifications and, in at least some educational agencies, may need to dedicate all or most of their time to the data privacy and security tasks. This commenter also referred to some of the NIST Framework’s provisions and stated that “… it appears to point to full-time work and there would most certainly be a cost to fill such a position.”

RESPONSE: No change is necessary. While the Department does not believe that an educational agency can completely outsource the job function of a Data Protection Officer and the proposed rule requires that an employee be assigned to this function, it does not prohibit the use of a third party such as a BOCES from providing some of the functions of that office. Moreover, the proposed rule provides that a current employee of an educational agency may perform this function in addition to other job responsibilities. It is not the expectation of the Department that the DPO would single-handedly perform all the activities in the NIST Framework. The Department will also provide guidance to assist educational agencies to meet the requirements, as needed.

36. COMMENT: Another commenter stated that the statement in the regulatory impact statement that “The proposed amendment does not impose any direct costs on local governments beyond those imposed by the statute” is untrue. They further

stated "…just as one example, the statute does not dictate the NIST CSF standards and districts, BOCES and vendors are not presently obligated to meet the requirements of those standards. There will most certainly be new costs imposed on educational agencies to meet the new NIST CSF standards if adopted. It is our view that the regulatory impact statement filed with the proposed regulation is insufficient under State Administrative Procedure Act § 202-a, and request that a new impact statement be filed that meets the requirements of that law.

RESPONSE: The proposed rule is consistent with the requirements of Education Law §2-d. Education Law §2-d requires that the commissioner, in consultation with the Chief Privacy Officer, to promulgate regulations that establish a standard for educational agency data security and privacy. The Department selected the NIST standard to implement the statutory requirements. The Department revised its Regulatory Impact Statement as part of its revised rulemaking in July to help clarify that due to the fact that the NIST standard is not a one size fits all standard and it has not been implemented in New York State, the Department does not have data that would enable to quantify an expected cost.

37. COMMENT: A commenter states that they disagree with the department's response to their comments on the Armed Services Vocational Aptitude Battery-Career Exploration Program (ASVAB) from the initial comment period are beyond the scope of the proposed regulation and urge the department to harmonize the obligations imposed on New York schools to permit military recruiter access to student directory information with the protections under Education Law §2-d and the proposed regulation.

RESPONSE: No change is necessary as this comment is beyond the scope of rulemaking.

38. COMMENT: A commenter writes that it is imperative for the Department to more carefully address the use of biometric surveillance technology and the best solution would be to include in the proposed regulation a moratorium on the use of biometric surveillance in schools.

RESPONSE: The Department is aware of the concerns raised about the use of technology that utilizes biometric data in schools and continues to research and review these issues. No change is necessary.

39. COMMENT: A commenter writes that they support the additions to section 121.6, of the proposed regulation which clarify the required elements of the data security and privacy plan. They believe such plans should be made publicly available. They are also supportive that the proposed regulation adopted their recommendation to include explicit prohibitions on certain types of data being shared.

RESPONSE: Since the comment is supportive, no change is necessary.

40. COMMENT: A commenter writes that the bill of rights should specifically include the Protection of Pupil Rights Amendment (PPRA), the National School Lunch Act (NSLA) and the Children's Online Privacy Protection Act (COPPA) and should also include the section in Education Law §2-d which provides the Chief Privacy Officer with the authority to expand the Parent Bill of Rights in the future, as threats to

student privacy and cybersecurity are likely to grow. The commenter also suggest that personally identifiable information of former students and teachers as well as current students and teachers should be covered under the proposed regulation as well. The commenter writes that the regulation should also include the specific provision in Education Law §2-d that bars districts from reporting to the state any data regarding (1) juvenile delinquency records; (2) criminal records; (3) medical and health records; and (4) student biometric information, except as required by law or required enrollment data. The commenter writes that in order to collect personal data, vendors should be required to have written contracts with the education agencies and must be responsible for making sure that this data is available to parents upon requests. They suggest that the word “license” should be added to the section on the Bill of Rights and in the section that prohibits districts and/or their contractors from selling personal student data, so that third-party contractors are barred from selling and/*or* licensing student data for a fee. Additionally, the commenter suggests that vendors and third-party contractors should be explicitly barred from selling data in the case of a bankruptcy. The commenter also states that education agencies should be required to publish their data and security privacy policies on their websites and provide notice of these policies to parents, not just employees; they should be required to post all contracts with vendors who collect student data, which should specify which categories of personal student data they are collecting and how parents may request access to such data; and education agencies should have to explain what the educational purpose is for allowing vendors access to this data. Finally, the commenter writes that data breach notification to parents and affected parties should be carried out by regular

mail as well as email; not phone calls, and that the regulations should incorporate all the powers and responsibilities of the Chief Privacy Officer as stated in Education Law §2-d.

RESPONSE: There is no statutory requirement that the parent bill of rights for data privacy and security incorporate the referenced federal laws. With regards to student data, the proposed rule adopts FERPA's definition of personally identifiable information. Teacher and principal data is defined to mean the records of an educational agency relating to the annual professional performance reviews of classroom teachers or principals that is confidential and not subject to release under the provisions of Education Law §§3012-c and 3012-d. With regards to the comment about including specific language from Education Law §2-d in the proposed rule, that provision is in §121.2 (d). Regarding the request to require regular mail be used for notifications, the proposed rule provides minimum requirements for notification, but educational agencies may exceed these and provide notification through additional means. While the proposed rule does not explicitly require notice of the data security and privacy policy to be provided to parents, it requires the policy to be published on each educational agency's website. With regards to the comment that vendors should be required to have written contracts with the education agencies, both the statute and the proposed rule define a third-party contractor as "... any person or entity, other than an educational agency, that receives student data or teacher or principal data from an educational agency pursuant to a contract or other written agreement for purposes of providing services to such educational agency, including but not limited to data management or storage services, conducting studies for or on behalf of such

educational agency, or audit or evaluation of publicly funded programs." Further, Education law Section 2-d provides that personally identifiable information maintained by educational agencies, including data provided to third-party contractors and their assignees, shall not be sold or used for marketing purposes. The proposed rule implements Education Law §2-d and is consistent with its provisions. No change is necessary.

41. COMMENT: A commenter writes that school districts have limited budgets and resources and to expect them to individually protect their data is not realistic. The commenter suggests the Department should vet some major vendors that can help with the protection of data and disaster recovery implementations and once these vendors are vetted and in place, then districts can work directly with them.
RESPONSE: The proposed rule implements Education Law §2-d. No change is necessary.

42. COMMENT: A few commenters write that NIST is working on a new privacy framework that more closely aligns with the Department's goals regarding data privacy. They question if and how the Board of Regents plan on incorporating the new NIST privacy framework.
RESPONSE: The proposed amendment requires educational agencies to comply with the NIST standards. Therefore, the Department does not believe any change is warranted.

43. COMMENT: Another commenter writes that the consent required in Section 121.9(a)(5) of the proposed regulation should include a requirement for prior written consent of affected teachers and/or principals as well as parents or eligible students. The commenter also suggests that Section 121.9(a)(8) should permit the educational agency to consent to disclosures that may technically fall within such provision, but which are part of a school-approved service or program. They write that without such clarifications such provision may conflict with Section 121.9(a)(4) and require parent consent for educational programs that are otherwise permitted under FERPA and undertaken with the consent of the agency.

RESPONSE: The proposed rule implements Education Law §2-d and has been revised to remove the parental consent requirement under section 121.9(c), therefore no change is necessary.

44. COMMENT: A commenter writes that they are concerned that if parental consent requirements are imposed without more evaluation and study, and without realistic protocols and timelines, this would be problematic for all involved. They suggest that any parental consent requirements should also require the department to issue guidance on how districts/schools can implement the consent requirement while ensuring that underrepresented students do not lose out on postsecondary opportunities and scholarships. They also suggest requiring a study to evaluate and make recommendations to improve parental consent participation rates and another more long-term study to determine the impact of the parent consent provisions on college-going rates.

RESPONSE: The proposed rule implements Education Law §2-d and has been revised to remove the parental consent requirement under section 121.9(c), therefore no change is necessary.

46. COMMENT: A commenter writes that in the previous comment period they submitted comments that remain unaddressed. Specifically their comment stating that the proposed regulation has a selective and incomplete list of duties of the Chief Privacy Officer, and their comment stating that the NIST CSF data security and privacy standard is designed for individual businesses and other organizations to assess enterprise risks they face in the conduct of their business and that it is not designed to ensure that confidential information is protected and remains confidential. The commenter writes that there are other NIST standards that may be more appropriate, or another alternative would be to utilize the U.S. Department of Education Privacy Technical Assistance Center ("PTAC) and the Student Privacy Police Office's "Data Security Checklist".

RESPONSE: No change is necessary. The functions of the chief privacy officer enumerated in Education Law §2-d are required by State statute and need not be enumerated in the proposed regulation. Additionally, as previously stated the NIST Cybersecurity Framework is recognized nationally and used internationally as a flexible, cost-effective and risk-based standard that helps entities protect their critical or sensitive infrastructure. The NIST Standards do not apply to one specific sector and therefore the Department believes the standards are applicable to school settings.

ATTACHMENT C

ASSESSMENT OF PUBLIC COMMENT

Following publication of the Notice of Proposed Rule Making in the State Register on January 30, 2019, the Department received the following comments on the proposed amendment. These comments were previously published as part of the July 2019 Board of Regents Item

§121.1 – Definitions

1. COMMENT: Commenters requested changes to the definition of “data breach” in §121.1(a) to align with New York’s data breach notification law.
RESPONSE: No change is necessary. The definition of breach in the General Business Law §899-aa is not specific to educational agencies and does not specifically address personally identifiable information, as defined in Education Law §2-d.

2. COMMENT: A few commenters were concerned that the definition of “Commercial and Marketing Purpose” in the proposed rule might preclude the offering of college
search services to students and parents who consent to the release of college entrance test data to colleges and higher education institutions by college admissions testing companies. This data is used to target mailings to students about higher educational opportunities, and some of the comments expressed concern about the impact imposing limitations on this activity could have on

traditionally under-served communities. One commenter noted that “families consent and opt-in to receive these notifications and services, and that any limitation of these services would be outside the intent of Education Law §2-d.” Some commenters recommended §121.1(c) be amended to include an exemption from the definition of Commercial or Marketing Purpose for nonprofit organizations engaging in activities to provide students with higher education and scholarship opportunities.

RESPONSE: The Department revised §121.9 to add a section that provides that where a parent or eligible student requests a service or product from a third-party contractor and provides express consent to the use or disclosure of personally identifiable information by the third-party contractor for purposes of providing the requested product or service, such use by the third-party contractor shall not be deemed a marketing or commercial purpose prohibited by the proposed rule. The Department believes that this revision addresses that concern.

3. COMMENT: A commenter requested that the definition of “Commercial or Marketing Purpose” be amended to delete the words “develop and improve” from the definition, or alternatively, to add language to the definition that states that the definition does not apply to “use or disclosure of student data to the extent that is used to develop or improve educational products or services.” The commenter indicates that such a change would reconcile the proposed rule with the laws of other ‘SOPIPA states’ which expressly allow the use or disclosure of student data

to develop new or improved educational products or services. The commenter stated that without this change, the proposed rule may bar all use or disclosure of student data for this “very positive” purpose.

RESPONSE: Education Law §2-d provides specific requirements for protecting personally identifiable information and does not provide for such an exception. Typically, aggregate, anonymized or de-identified data (which is data from which identifiable information has been permanently removed with no chance of reidentification) is the type of data used to develop or improve products or services, and not personally identifiable information. Every use of personally identifiable information by a third-party contractor must comply with the requirements of Education Law §2-d and the proposed rule.

4. COMMENT: A commenter recommended a revision to the definition of “Commercial

or Marketing Purpose” to add language which clarifies that the definition does not encompass corporate merger and acquisition activities of third-party contractors such as the purchase, merger, or other type of acquisition of a third-party contractor by another entity, where the successor entity continues to be subject to the provisions of Part 121 with respect to previously acquired student information.

RESPONSE: No change is necessary. The protections outlined in Education Law §2-d apply to personally identifiable information even where the corporate structure of an entity changes.

5. COMMENT: Several commenters were concerned that the definition of “contract or other written agreement” could limit the use of software applications that do not comply with the proposed rule’s requirements for contracts with third-party contractors.

RESPONSE: No change is necessary. The proposed rule is consistent with Education Law §2-d.

6. COMMENT: A commenter stated that the definition of “school” inappropriately includes charter schools, stating that §2854(1)(b) of the New York Charter Schools Act exempts charter schools from most state rules outside of health, safety, civil rights and student assessment requirements.

RESPONSE: No change is necessary. The proposed rule is consistent with Education Law §2-d. Education Law §2854 (1)(b) specifically provides that a charter school shall meet the same health and safety, civil rights, and student assessment requirements applicable to all other public schools. Education Law §2-d protects personally identifiable student data, which includes highly personal and sensitive information related to students. The requirements related to the protection of such data contained in Education Law §2-d are therefore related to health and safety as well as civil rights. Therefore, the Department’s position is that the Education Law §2-d and the proposed rule apply to charter schools.

7. COMMENT: A commenter requested that the Department adopt its own definition of personally identifiable information that is separate from the definition in the Family Educational Rights and Privacy Act (FERPA).

RESPONSE: The definition of personally identifiable information in the proposed rule is consistent with statutory definition. Therefore, the Department believes no change is necessary.

8. COMMENT: A commenter recommended that the Department define “Encryption Technology” to mean “technology referenced by the Secretary of the United States Department of Health and Human Services in guidance issued under Section 13402(H)(2) of Public Law 111-5.”

RESPONSE: The Department has revised the proposed rule to add a new definition for “Encryption” as follows: “methods of rendering personally identifiable information unusable, unreadable, or indecipherable to unauthorized persons through the use of a technology or methodology specified or permitted by the Secretary of the United States department of health and human services in guidance issued under Section 13402(H)(2) of Public Law 111-5.”

9. COMMENT: A commenter wrote that the use of applications that require "click wrap" agreements by teachers and other educators will be significantly limited or eliminated because “they are offered by vendors who don't meet the third-party vendor requirements of Education Law 2D”. Another commenter raised the issue of educational agency compliance when utilizing systems pursuant to a click-wrap agreement and expressed concern that educational agencies may “not be able to use these systems at all, or there could be a great deal of work involved in compliance.” The commenter requested additional discussions be held on this

issue.

RESPONSE: No change is necessary. The requirements of the statute apply regardless of the form of contract utilized and making an exception from compliance merely based on the form of contracting would not align with the purpose of the statute to protect personally identifiable information. The Department acknowledges the issues raised regarding such agreements, and will provide guidance, as needed, to assist educational agencies in meeting the requirements of the proposed rule.

10. COMMENT: A commenter requested that we add “former student” to the definition of “student.”

RESPONSE: No change is necessary. The proposed rule adopts Education law §2 d’s definition.

11. COMMENT: A commenter wondered why the Department did not define “educational purpose” in the proposed rule.

RESPONSE: Education Law §2-d does not provide a definition for “educational purpose.” Therefore, no change is necessary. The Department could address this in future guidance if needed.

12. COMMENT: A few commenters wanted additional clarification on how Personally Identifiable Information is different from Directory Information. Another Commenter requested that the Department amend the definition of Personally Identifiable Information in §121.1 to explicitly include Directory Information.

RESPONSE: No change is necessary. The proposed rule adopts Education Law §2-d's definition of personally identifiable information. The Department will provide additional guidance and model documents to provide further clarification to educational agencies on meeting the requirements of the proposed rule.

§121.2 Educational Agency Data Collection Transparency and Restrictions.

13. COMMENT: A commenter wrote to express support for the language in §121.2(b) relating to data minimization, collection, processing, and transmission. The commenter encouraged the Department to provide training resources to schools to educate teachers and administrators on best practices and standards for data minimization techniques, "particularly regarding sensitive information categories such as the information of children, work review information, financial data, and health information, among others." The commenter highlighted issues regarding school transmission of personally identifiable information on social media platforms and recommended that the Department make specific social media training available to schools that will facilitate school personnel learning how to draft and implement appropriate data minimization policies for schools-- including those relating to social media platforms.

RESPONSE: No change is necessary as the comment is supportive. The proposed rule requires educational agencies to provide annual data privacy and security training to their employees.

14. COMMENT: A commenter noted that the proposed rule should include the provisions in Education Law §2-d that provide that “school districts shall not report to the Department the following student data elements:(1) juvenile delinquency records;(2) criminal records;(3) medical and health records; and (4) student biometric information unless required by law except in the case of law or required educational enrollment data.”

RESPONSE: The Department made this revision to the proposed rule.

15. COMMENT: A commenter strongly supported the language in §121.2(a) and urged

the Department to retain it with no changes because they interpreted it as “a blanket prohibition of the sale of identifiable student data as defined by Education Law §2-d, inclusive of FERPA directory information held by the school for which parents did not supply an opt-out.” The commenter believed this language would prevent sales or sharing of student data to data brokers, which they thought was positive.

RESPONSE: No change is necessary. The comment is supportive.

§121.3 Bill of Rights for Data Privacy and Security.

16. COMMENT: A commenter requested clarification on whether the parent’s bill of rights will be provided by the Educational Agency or by Third Party Contractor.

RESPONSE: No change is necessary. Education Law §2-d requires each educational agency to develop and publish its parent’s bill of rights on its website.

17. COMMENT: A commenter noted that it could be a security risk to require educational agencies to publish information about contracts and third parties publicly on the agency's websites as it may allow hackers easy access to information about the third-party contractors that receive student data to provide services to an educational agency. The commenter suggested the use of a parent portal or newsletter to meet this requirement as an alternative.

RESPONSE: No change is necessary. The proposed rule gives educational agencies the discretion to determine when data should be redacted to protect the privacy and security of the educational agency's data or technology infrastructure.

18. COMMENT: A commenter stated that "the requirement for each educational agency

to adopt a parent's bill of rights for data privacy and security that is included with every contract an educational agency enters with a third-party contractor that receives personally identifiable information and that is published on its website, will limit the technology that teachers and students can use, even if it is FERPA and COPPA compliant." The commenter stated that students will no longer be able to immediately utilize different apps when working on projects and researching information in a timely manner and that it will cause student innovation to suffer greatly.

RESPONSE: No change is necessary. The proposed rule is consistent with Education Law §2-d's provisions.

19. COMMENT: A commenter expressed concern that vendors for multi-year software
contracts will not be Education Law §2-d compliant.

RESPONSE: No change is necessary. Education Law § 2-d is clear that third party contractors must comply.

20. COMMENT: A commenter requested that the Department clarify the responsibility
of subcontractors to comply with the data protection and security requirements imposed on the third party contractor, and requested that the Department add a provision that requires third party contractors to prohibit their subcontractors from using student data or teacher or principal data for any purpose other than for providing the contracted service, and that prohibits redisclosure.

RESPONSE: No change is necessary. The Department believes that the proposed rule is clear with regard to the requirements of third-party contractors to assure their subcontractors are in compliance with the requirements of the statute and the proposed rule.

21. COMMENT: A commenter stated that this section should specifically reference the following federal laws: Protection of Pupil Rights Amendment (PPRA), National School Lunch Act (NSLA) and Children's Online Privacy Protection Act (COPPA).

RESPONSE: No change is necessary. There is no requirement that the proposed rule reference every related federal law. These federal laws apply regardless of

whether they are specifically mentioned in the proposed rule.

22. COMMENT: A commenter notes educational agencies should be required to post all contracts with vendors that receive personal student data on their website, and identify the data element received, or make the contracts available for review upon request and communicate how parents may request access.
RESPONSE: No change is necessary. The proposed rule requires educational agencies to publish their parent's bill of rights and supplemental information for each contract (including information such as the purpose for which the data will be used, how the data will be protected, the duration of the contract, how a parent, student or eligible student may challenge the accuracy of the data collected, and what will occur to the data upon expiration of such contract) on each agency's website. Further, nothing in the proposed rule prohibits educational agencies from providing access to contracts to their stakeholders.

23. COMMENT: A commenter recommended that §121.3(c)(3) be revised to add a requirement that where data held by a third-party contractor is not destroyed upon expiration of a contract, it must be returned to the educational agency.
RESPONSE: No change is necessary as the proposed rule's current language allows for either the destruction of data or its return to the educational agency. Each educational agency may elect its preference as part of the contracting process.

24. COMMENT: A commenter indicated broad support for §121.3. The commenter recommended removing the examples in §121.3(c)(5) to avoid any potential

interpretation that this section is promoting a specific type of data storage option, and to keep the proposed rule from becoming outdated as technology develops.
RESPONSE: Revision made. The Department has removed the examples from §121.3(c)(5).

25. COMMENT: A commenter requested that the references to encryption in §121.3(6)
and §121.9 of the proposed rule use consistent language to avoid confusion.
RESPONSE: “Encryption” is now defined in §121.1 and referenced in §121.1(3)(c)(6) and §121.9(6) also now references “encryption” and reads: “(6) address how the data will be protected using encryption while in motion and at rest.” The Department believes that these changes address the commenter’s concern.

26. COMMENT: A commenter requested that this section require educational agencies
to identify whether a parent could opt out of an educational agency’s data collection. Another commenter requested that this section provide that the Department must not collect personally identifiable data on individual students related to their country of birth and in-school or out-of-school suspension.
RESPONSE: No response is necessary. The changes requested are beyond the scope of Education Law §2-d and the rulemaking process.

27. COMMENT: A Commenter stated that §121.3 of the proposed rule should

incorporate the following language from Education Law §2-d(4)(e): “Except as required by law or in the case of educational enrollment data, school districts shall not report to the Department the following student data elements: (1) juvenile delinquency records; (2) criminal records; (3) medical and health records; and (4) student biometric information.”

RESPONSE: The Department has made this change to mirror the statutory language.

28. COMMENT: A commenter requested that the Parent's Bill of Rights explicitly state that directory information is protected under Education Law §2-d regardless of whether a parent submitted a Directory opt-out form or not.

RESPONSE: No change is necessary. The changes requested are beyond the scope of Education Law §2-d and the rulemaking process.

29. COMMENT: A commenter wanted the word “if” removed from section 121.3(c)(4) – which states “…if and how a parent, student, eligible student, teacher or principal may challenge the accuracy of the student data or teacher or principal data that is collected.”

RESPONSE: No change is necessary. The language of the proposed rule mirrors Education Law §2-d.

30. COMMENT: A commenter requested a requirement that third-party contractors identify all subcontractors that will be utilized to provide contract services or products in the supplemental information for each contract.

RESPONSE: No change is necessary. The proposed rule does not preclude educational agencies from including or requiring this information in the supplemental information for their contracts with third party contractors.

§121.4 Parent Complaints of Breach or Unauthorized Release of Personally Identifiable Information

31. COMMENT: A commenter recommended that §121.4 should provide that complaints be submitted in writing, and investigation findings provided by the educational agency should also be in writing. The commenter also requested that the Commissioner develop a standardized complaint form.

RESPONSE: Revision made in part. The Department added §121.4(d) which states "…Educational Agencies may require complaints to be submitted in writing." The request that the Department develop a standardized complaint form, is outside the scope of this rulemaking and no changes were made in this regard. However, the Department will provide guidance and model documents to assist educational agencies in meeting the requirements.

32. COMMENT: A commenter recommended that §121.4(c) limit the time an educational agency could have to respond to a complaint to 6 months from the date the complaint is received.

RESPONSE: No change is necessary. Education Law §2-d provides educational agencies with the flexibility to fully investigate each complaint. It cannot be determined with certainty how long each complaint will need to be fully investigated and resolved.

33. COMMENT: A commenter recommended that this section be clarified to ensure that records of data breaches would be made available to the public through FOIL and redacted as appropriate prior to release.

RESPONSE: No change is necessary. The changes requested are beyond the scope of Education Law §2-d and the rulemaking process.

§121.5 Data Security and Privacy Standard

34. COMMENT: A commenter wrote that they believed the “Drafting Workgroup rejected the more protective NIST SP 800-171 standards in favor of the NIST Cybersecurity Framework because the subject matter was beyond the technical understanding of the members.”

RESPONSE: The selection of the NIST Framework was reviewed by experts in the field, the Chief Privacy Officer’s Technical Standards Selection Workgroup and the Implementation Workgroup. While the team originally selected the NIST 800-171 because it met the 5 qualities the group found desirable in a standard (it was credible, durable, enforceable, understandable and supportable). In conversations with the field and national experts, the Chief Privacy Officer decided to consider the newer NIST Framework as an option to mitigate the confusion about the applicability of the NIST 800-171 to the education sector as it was originally developed for federal government contractors. The Chief Privacy Officer also wanted a standard that had two additional qualities – flexibility and simplicity. She asked the Implementation Workgroup to work with the field to compare both

standards and select one. The selection of the NIST Cybersecurity Framework was ultimately a decision made by the workgroup.

35. COMMENT: A few commenters stated that some sub-categories of the NIST Cybersecurity Framework that apply to controls around suppliers and the supply chain may not be applicable to the K-12 educational sector and gave examples of certain sub-categories in the Framework that reference a supply chain; one of the commenters acknowledged that they had heard from technical experts that implementing the NIST CSF would certainly have some benefit and that many of the standards can be implemented if educational agencies are given the appropriate amount of time and the financial resources to do so. Another commenter thought the Framework was not designed to ensure that confidential information is protected and remains confidential, and recommended other standards be considered such as the NIST SP 800-17, NIST's Guide to Protecting the Confidentiality of Personally Identifiable Information, and the U.S. Department of Education Student Privacy Policy Office's "Data Security Checklist.
RESPONSE: See response to Comment #34. No change is necessary. The NIST Cybersecurity Framework is a flexible standard that is intended to be tailored to different sectors such as the education sector. The Department will provide implementation guidance to the field as needed.

36. COMMENT: A commenter stated that the proposed rule refers to two different security standards –the NIST Cybersecurity Framework and the HIPAA encryption standard. The commenter noted that while there is some alignment between the

standards, they do have different requirements. The commenter expressed concern that these requirements may cause confusion for school staff or third-party contractors and recommended that the Department provide technical assistance for educational entities.

RESPONSE: No change is necessary as the referenced standards are complementary and are not conflicting. Education Law §2-d provides that encryption should be performed using a technology or methodology specified or permitted by the Secretary of the United States department of health and human services in guidance issued under Section 13402(H)(2) of Public Law 111-5. The NIST Cybersecurity Framework 1.1 specifies controls but builds in flexibility regarding adoption of specific controls. We do not see a conflict between both. The Department will provide guidance to assist educational agencies in meeting the requirements of the proposed rule, as needed.

37. COMMENT: A commenter stated the NIST Cybersecurity Framework is too restrictive and is concerned that there will be fewer service offerings to students if educational agencies may only use vendors that align with it. The commenter noted that its company utilizes ISO 27001, and wondered if third party contractors can comply with the proposed rule using a comparable framework such as the ISO 27001.

RESPONSE: No change is necessary. The proposed rule requires third-party contractors to align to the NIST Cybersecurity Framework. The requirements of the NIST Cybersecurity Framework can be fulfilled using other standards which the framework references as informative references. One of those informative

references is the ISO 27001. Those informative references can be used to address the categories and sub-categories identified in the Framework.

38. COMMENT: A commenter requested that access to the Department's model policy be available prior to the date educational agencies must adopt their own data security and privacy policy.

RESPONSE: No change is necessary. The Department will provide a model data security and privacy policy as provided in Education Law §2-d prior to the date that educational agencies must adopt their policies, that educational agencies may use as a guide to develop their own policies.

39. COMMENT: A commenter recommended a revision of §121.5(c) to add language that clarifies that personally identifiable information should not be included in public reports or documents regardless of whether those documents are online or offline.

RESPONSE: No change is necessary. The proposed rule prohibits the publication of personally identifiable information in public documents.

40. COMMENT: A commenter recommended that this section mandate that Directory Information opt out forms be included in the educational agency's Data Security and Privacy Policy.

RESPONSE: No response is necessary. The comment is beyond the scope of Education Law §2-d.

41. COMMENT: Several commenters stated that the proposed timeline is too aggressive and requested additional time to implement the proposed rule.
RESPONSE: Revision made in part. The Department has revised the date by which educational agencies must adopt and publish a data security and privacy policy specified in §121.5 to July 1, 2020 to give educational agencies additional time to implement the requirements of the proposed rule.

42. COMMENT: A commenter stated that hiring an outside security company/ expert has provided his agency with valuable information on a yearly basis and recommended that this be practice be required “in lieu of parts of the NIST Framework.”
RESPONSE: Every educational agency is responsible for ensuring that their data security and privacy policies and practices align with the requirements of Education Law §2-d and the proposed rule. The proposed rule does not prohibit the use of outside experts to assist educational agencies with their compliance activities.

43. COMMENT: A commenter suggested that “BOCES can provide a recommended list of security engineers and companies.” The commenter also recommended that BOCES help negotiate with large third-party contractors to ensure compliance with the NIST Cybersecurity Framework, and also maintain a list of educational software products that are compliant. The commenter also stated that “if BOCES has a service/software package on its statewide contract, the contract, when it comes up, should require compliance with Ed Law IID so it is done one time for the entire state. Then districts save time, and the companies get one

request." The comment also stated that the "state could do a survey of which 3rd parties are used and negotiate directly with vendors to ensure compliance and avoid countless hours of duplicate labor."

RESPONSE: No change is necessary. The proposed rule does not prohibit school districts from seeking assistance from BOCES, consistent with Education Law §1950.

44. COMMENT: A commenter recommended revising §121.5)(c)(1) to include the word 'disclosure.'

RESPONSE: This revision was made.

45. COMMENT: One commenter requested that the Department include a requirement that an educational agency's data security and privacy policy "shall include all the protections afforded to parents or eligible students, where applicable, under FERPA and the Individuals with Disabilities Education Act (20 U.S.C. 1400 et seq.), and the federal regulations implementing such statutes."

RESPONSE: No change is necessary. There is no requirement that the proposed rule reference federal laws that relate to privacy and confidentiality. These federal laws apply regardless of whether they are specifically mentioned in this Rule.

46. COMMENT: A commenter stated that because the NIST Cybersecurity Framework may be updated by the U.S. Department of Commerce over time, the regulations should say that these requirements may themselves be updated regularly.

RESPONSE: No change is required. The Department is adopting the most current version of the NIST Cybersecurity Framework available at this time. Further, as part of the rulemaking process, documents referenced or incorporated into a rule must be filed with the Department of State and for this reason, it cannot be left open-ended for future versions, and still meet the requirements of Executive Law §102(1)(c).

47. COMMENT: A commenter requested that this section should require each educational agency to provide notice of its Data Security and Privacy Policy to parents as well as employees.

RESPONSE: No change is necessary. While the proposed rule does not explicitly require notice of the data security and privacy policy to be provided to parents, it requires the policy to be published on each educational agency's website.

§121.6 Data Security and Privacy Plan.

48. COMMENT: Several commenters requested that the Department develop a centralized list of approved software applications or, negotiate compliant contracts with third-party contractors. Commenters believed this would avoid an unnecessary duplication of efforts by districts. More specifically, a commenter welcomed the "stringent comprehensive requirements" but felt that "asking every single school district to have every vendor sign off on a contract including an addendum regarding how they are going to use student data is onerous to both the district and the vendors." The Commenter wondered if the contracting could be better administered at either the state level or at the regional level by the Regional

Information Centers.

RESPONSE: No change is necessary. The requested change is outside the scope of Education Law §2-d and the proposed rule.

49. COMMENT: A commenter asked whether the Department contacted the vendor community to determine their willingness and/or ability to comply with the proposed rule.

RESPONSE: The 14 public forums that the Department held across the state to seek feedback from stakeholders were open to all, and representatives from a few vendor companies attended. The Department also received comments from some members of the private sector during the 60-day public comment period. In addition, a representative from the Future of Privacy Forum (FPF) participated on the DPAC and provided feedback from the vendor community, as this organization engages extensively with many members of the vendor community and was able to provide some feedback from the vendor perspective. To be clear, the requirements imposed upon third party contractors are statutorily required, and the proposed rule implements Education Law §2-d.

50. COMMENT: A commenter requested guidance as to whether educational agencies

are required to recover data from vendors at the end of a contract and if so, how long such data should be maintained by the educational agency.

RESPONSE: §121.3(c)(3) and 121.6(a)(6) both include provisions that address how the contract with a third-party contractor should address transitioning of data to

the educational agency or its designee at the end of the contract. Regarding the retention of data by an educational agency, retention should be maintained in accordance with applicable rules such as the Records Retention and Disposition Schedule ED-1 (8 NYCRR (Appendix I)).

§121.7 Training for Educational Agency Employees.

51. COMMENT: A commenter inquired about the recommended length of training and stated that “if you add the number of hours of mandated training by NYSED, school days will need to be altered.” The commenter requested that the Department provide an online training for all districts that is no longer than 5 minutes long.

RESPONSE: No change is necessary. The proposed rule does not stipulate the duration of annual training. To ensure that educational agencies have the flexibility to determine how to present appropriate training to staff in a meaningful, effective and efficient way, the proposed rule states that training may be delivered using online training tools and may be included as part of training the educational agency already offers to its workforce.

52. COMMENT: A commenter requested that the proposed rule specify the type of training educational agencies must provide and suggested that this section require that training should include the NIST Framework standards and cybersecurity protocols. Another commenter recommended including training on breach notification mechanics, Directory Information, and health data protections pursuant to FERPA and HIPAA.

RESPONSE: Revision made in part. The proposed rule has been revised to state that training should be provided on, among other things, “the state and federal laws that protect personally identifiable information, and how employees can comply with such laws.”

§121.8 Educational Agency Data Protection Officer

53. COMMENT: A commenter asked the Department to “extend the timeline for implementation by one year allowing adequate time to get in place the best person for the position (certification, experience, etc.)” and allow more flexibility with regard to qualified applicants by eliminating the administrative certification/requirement that the DPO hold an administrative degree.

RESPONSE: The proposed rule does not require that the DPO hold an administrative degree or certification. While the proposed rule does contain a timeline by which educational agencies must adopt and publish a data security and privacy policy specified in §121.5, this has been extended to July 1, 2020 to give educational agencies additional time to implement the requirements of the proposed rule (see response to Comment #41).

54. COMMENT: Some commenters suggested that the Department permit external parties such as private entities and BOCES to provide some of the functions of the Data Protection Officer. The commenter believed this could assist small and rural educational agencies. Another commenter did not believe that an employee could perform the duties of a DPO in addition to other job responsibilities. A different

commenter stated that districts may not have a current employee with the requisite knowledge and experience to do the work that this law requires, and/or may not have the financial capacity to cover any additional costs without having to cut an already existing essential staff or program. One commenter stated that they would like to see a CoSer for this position. Another commenter stated that "instituting a DPO by December 2019 will present significant implementation challenges." Another commenter highlighted the fact that the DPO would need to have a unique set of qualifications and, in at least some educational agencies, may need to dedicate all or most of their time to the data privacy and security tasks. This commenter also referred to some of the NIST Framework's provisions and stated that "… it appears to point to full-time work and there would most certainly be a cost to fill such a position."

RESPONSE: No change is necessary. While the Department does not believe that an educational agency can completely outsource the job function of a Data Protection Officer and the proposed rule requires that an employee be assigned to this function, it does not prohibit the use of a third party such as a BOCES from providing some of the functions of that office. Moreover, the proposed rule provides that a current employee of an educational agency may perform this function in addition to other job responsibilities. It is not the expectation of the Department that the DPO would single-handedly perform all the activities in the NIST Framework. The Department will also provide guidance to assist educational agencies to meet the requirements, as needed.

§121.9 Third Party Contractors

55. COMMENT: A commenter requested that nonprofit organizations be exempted from complying with the requirements of this section.

RESPONSE: No change is necessary. The rule as proposed is consistent with Education Law §2-d, which contains no provision exempting nonprofit organizations.

56. COMMENT: A commenter recommended a change to §121.9 to clarify that the sale

of student and class photographs or yearbooks pursuant to a contract with an educational agency is not prohibited commercial or marketing activity.

RESPONSE: No change is necessary. While contracts with third-party contractors must comply with the regulations, nothing in the proposed rule prohibits the sale of student and class photographs or yearbooks pursuant to a contract with an educational agency.

57. COMMENT: A commenter recommended prohibiting the licensing of student data

and stated that there is no significant difference between selling and licensing data.

RESPONSE: No change is necessary. Education Law §2-d is clear in its prohibition of the use of personally identifiable information for any commercial or marketing purpose, which the proposed rule (as revised) defines as “the sale of student data; or its use or disclosure for purposes of receiving remuneration, whether directly or indirectly; the use of student data for advertising purposes, or to develop, improve or market products or services to students.” This would include licensing data.

58. COMMENT: A commenter recommended that this section require that third party
contractors provide written assurances of compliance with the data security and privacy policy of the educational agency.
RESPONSE: No change is necessary. Third party contractors are required by the proposed rule to comply with the educational agency's Data Security and Privacy Policy. Nothing limits the ability of educational agencies to require written assurances or warranties in their contracts.

59. COMMENT: A commenter recommended that language requiring the prior written
consent of a parent or eligible student prior to the release of any Personally Identifiable Information by a third-party contractor should be expanded to include teacher and principal APPR data pursuant to §121.9(a)(4)(ii).
RESPONSE: The statute does not contemplate this, and the proposed rule mirrors the statute. As such, no revision is necessary.

60. COMMENT: A commenter requested that this section include language that would
explicitly allow the transfer of personally identifiable information as part of an asset purchase or acquisition of any part of a service provider by another entity.
RESPONSE: No change is necessary. The regulatory language conforms to Education Law §2-d.

61. COMMENT: A commenter suggested a revision which specifies that the protections

of Education Law §2-d apply to any contractual relationship established prior to the proposed rule's effective date. Another commenter stated that the proposed rule would permit educational agencies to structure contractual arrangements to avoid compliance with Education Law §2-d and recommended it be revised to provide that NYSED will audit contracts to ensure they are structured appropriately to comply with the student data privacy protections set forth in Education Law §2-d and the proposed rule.

RESPONSE: The proposed rule implements Education Law §2-d. Regardless of the effective date of the rule, the relevant provisions of Education Law §2-d have been in effect and applicable to educational agency contracts since March 31, 2014. These obligations extend to sub-contractors as well. The Department does not believe that the requirements of the statute and the proposed rule can be avoided through contractual arrangements. Therefore, no change is needed.

62. COMMENT: A commenter requested clarification on the difference between §121.9(a)(2) which "limit[s] access to personally identifiable information to only those employees or sub-contractors that need access to provide the contracted services" and §121.9 (a)(4) which states "except for authorized representatives of the third-party contractor such as a subcontractor or assignee to the extent they are carrying out the contract and in compliance with state and federal law, regulations and its contract with the educational agency, not disclose any personally identifiable

information to any other party…"

RESPONSE: This section of the proposed rule has been revised overall for clarity. To respond to the comment, §121.9(a)(2) seeks to limit "internal" access to PII within a third party contractor's organization only to those employees or sub contractors who require it to provide the contracted service while §121.9(a)(3) is a prohibits third-party contractors from the re-disclosure of PII to parties outside of the organizations of the third-party contractor, its subcontractors, or assignees, without the prior written consent of a parent or eligible student, or pursuant to court order or statutory requirement under circumstances further detailed in the statute.

63. COMMENT: A commenter requested that the word "reasonable" be replaced with

"industry best practices" in §121.9(a)(5), which provides that third-party contractors must "maintain reasonable administrative, technical and physical safeguards to protect the security, confidentiality and integrity of personally identifiable information in its custody as prescribed by state and federal law, regulations and its contract with the educational agency."

64. RESPONSE: This section has been revised overall and renumbered and is now §121.9(a)(6) in the July 2019 version of the proposed rule. No change is necessary. The proposed rule is consistent with Education Law §2-d.

65. COMMENT: A commenter requested that the proposed rule exempt school attorneys, school physicians, school psychologists and other similar professional service providers from the requirements imposed upon third party contractors. The

commenter states that these providers are subject to professional rules of conduct such as the Model Rule of Professional Conduct applicable to attorneys, and the HIPAA Privacy Rule applicable to medical professionals.

RESPONSE: No change is necessary. Education Law §2-d addresses the security and privacy of personally identifiable information in educational agencies or provided to third-party contractors regardless of the size or professional affiliation of the contractor. The Department does not believe that the rules of professional conduct referenced, or other similar professional rules, including HIPAA, are equivalent substitutes for the data security and privacy requirements outlined in Education Law §2-d and the proposed rule for protecting personally identifiable student, teacher and principal information. Further, such an exception is not contemplated by Education Law §2-d and permitting it could jeopardize the privacy and security of the personally identifiable information and very sensitive data that these service providers receive from educational agencies.

§121.10 Reports and Notifications of Breach and Unauthorized Release

66. COMMENT: A commenter requested clarification regarding the format for notifying an educational agency of a breach by a third-party contractor to an educational agency. Another Commenter requested that this section state that where a BOCES

is the only other party to a contract with a third-party contractor, the educational agency and not the BOCES should assume the responsibility for notifying its own affected parties.

RESPONSE: No change is necessary. Notification procedures must be developed

by educational agencies in accordance with the requirements of Education Law §2 d and proposed rule. The Department will provide guidance to assist educational agencies.

67. COMMENT: A commenter requested that breach notifications to parents and affected parties should only be carried out by mail and that this section should not permit the use of email and phone notifications as alternatives. The commenter also recommended that notifications to data subjects recommend steps such individuals can take to mitigate the impact of a breach and include what actions the party responsible for the breach will take to mitigate its impact.
RESPONSE: No change is necessary. The proposed rule provides minimum requirements for notification, but educational agencies may exceed these and provide notification through additional means.

68. COMMENT: A commenter asked how much information should be provided to the public when notifications of incidents are made and expressed a concern about "parents who do not understand the technical realms and who have heightened sensitivity to any cyberattack and their child's privacy."
RESPONSE: No change is required. The proposed rule states that any required notification to parents, eligible students, teachers or principals required by this section must be "clear, concise, use language that is plain and easy to understand" and requires certain information to be provided. Among this required information is contact information for a representative who can assist parents or eligible students that have additional questions.

69. COMMENT: A commenter asked what would happen if a district could not meet its obligation to notify parents in a timely manner because a third-party contractor did not notify the district of the breach in a timely manner.

RESPONSE: Generally, third party contractors must notify educational agencies no more than seven calendar days after the discovery of a breach or unauthorized release. Pursuant to the proposed rule, the timeframe for educational agencies to notify affected parties is triggered upon their receipt of notification by the third-party contractor or discovery of the breach by the Educational Agency. The Chief Privacy Officer has authority to issue penalties to third party contractors where they are found to be in violation.

70. COMMENT: A commenter stated that they believed §121.10(b) and (d) to be duplicative provisions.

RESPONSE: The Department believes these provisions are not duplicative. We were making a distinction between breaches and unauthorized releases that are reported by the third-party contractor to the educational agency (§121.10(b)) and reports of breaches and unauthorized releases that are attributable to or discovered by the educational agency itself and are reported by the educational agency to the CPO (§121.10(d)).

71. COMMENT: A commenter requested that the benefit of the provision in §121.10(e) be extended to former students as well.

RESPONSE: No change is necessary as the proposed rule is consistent with

Education Law §2-d, which defines “student” as “any person attending or seeking to enroll in an educational agency” and “eligible student” as “a student eighteen years or older.” Education Law §2-d requires that an educational agency notify affected parents, eligible students, teachers and/or principals of a breach or unauthorized release of data. The Department will provide guidance to educational agencies, as needed, to assist them with this requirement.

72. COMMENT: A commenter asked that the proposed rule be expanded to cover breaches of other confidential and personally identifiable information that may be held by a third-party contractor on behalf of an educational agency such as banking, retirement, and investment information.

RESPONSE: No change is necessary. The regulatory language conforms to Education Law §2-d, and to the extent the information referenced by the commenter includes student data or teacher or principal data, it is covered by Education Law §2-d and the proposed rule.

§121.11 Third Party Contractor Civil Penalties

73. COMMENT: A commenter noted the proposed rule did not include the separate general penalty provisions of Education Law §2-d(7)(b) and recommended that it be added.

RESPONSE: Revision made. Language was added to mirror the provisions of Education Law §2-d to address this concern.

74. COMMENT: A commenter recommended that the Department revise §121.11 to state that penalties may only be imposed where the third party has breached or violated its duties with intent, recklessness or gross negligence. The commenter states that the use of “shall” in the section may be interpreted to mean that strict liability should apply for data breaches which does not recognize the fact that many data breaches can occur through no fault of a contractor, and recommended that the “shall” be changed to a “may” and language should be incorporated to clarify that it is applicable only to breaches that occurred with “intent, knowledge, recklessness or gross negligence”, consistent with Education Law §2d-6(e)(5).
RESPONSE: No change is necessary. The language of the proposed rule mirrors that of Education Law §2-d.

§121.12 Right of Parents and Eligible Students to Inspect and Review Students Education Records

75. COMMENT: A commenter requested that §121.12(d) be revised to state that a parent’s right to inspect and review their child’s education record under this section extends to “… any student data stored or maintained by a contractor on the agency’s behalf.”
RESPONSE: No change is necessary. The language of the proposed rule mirrors the statute., which includes “any student data stored or maintained by an educational agency.”

76. COMMENT: A commenter suggested that this section should make educational agencies responsible for arranging for records to be delivered to the parent or

eligible student. Another commenter also suggested an addition to §121.12(d) to include language requiring educational agencies to post FERPA or Directory Information opt out forms.

RESPONSE: The comment is outside the scope of the statute. As such, no response is necessary.

§121.13 Chief Privacy Officer's Powers

77. COMMENT: A commenter noted that ""privacy risk assessments" are better termed

"privacy impact assessments" (PIAs) and recommended that this change be made.

RESPONSE: Revision made in part. This section now references a "privacy impact and security risk assessment."

78. COMMENT: A commenter noted the rule should require the CPO's annual report to

be posted on the NYS Education Department's website by January 1 of each year and made available upon request.

RESPONSE: No change is necessary. Education Law §2-d provides that the functions of the Chief Privacy Officer shall include issuing an annual report on data privacy and security activities and progress and the law does not require that the report be posted on the Department's website by January 1 of each year. The CPO is working to develop a process for public dissemination of annual reports once adoption and implementation of the proposed rule occur.

79. COMMENT: A Commenter noted the Chief Privacy Officer had “too much authority” under Education Law §2-d and was concerned that the position was not defined enough to “know if they should have access to so much of our staff and student data.” Another commenter requested that this section be revised to include all the powers of the Chief Privacy Officer specified in Education Law §2-d(2)(c).
RESPONSE: Revision made in part. Regarding the comments that the Chief Privacy Officer “had too much authority under Education Law §2-d” and concerns expressed regarding the definition of her job duties, the rule as proposed is consistent with Education Law § 2-d. Regarding the comment that this section should mirror the statute and include all the Chief Privacy Officer’s powers outlined in the statute, the Department revised this section to include the additional powers of the chief privacy officer outlined in Education Law §2-d(2)(c).

General Comments

80. COMMENT: Commenters stated that the proposed rule should mandate that the CPO’s annual report be expanded to include a variety of metrics, including reporting on district compliance with Education Law §2-d and the proposed rule, data relating to the type of training received by school staff including the numbers, and roles of school staff trained, and a deadline for the completion and release of this annual report is recommended.
Some commenters noted the need for additional resources from SED including sample templates, model forms, guidance documents and model procedures. Commenters requested a sample Parent’s Bill of Rights, a sample Data Security and Privacy Policy, guidance to implement a Parent Complaint Process and

Incident Reporting and Notification forms. Another comment stated that the proposed rule should mandate educational agencies to provide parents with pre printed forms in their students' annual registration packet to permit easier parental participation in the opt-out process under ESSA/ESEA. A commenter requested a checklist of what educational agencies should be aware of when reviewing third party contracts.

RESPONSE: No change is necessary. The statute provides specific reporting requirements for the CPO and the proposed rule is consistent with the statute. The Department will provide guidance and model forms as needed to assist educational agencies in meeting the requirements of the proposed rule. To the extent that the commenter stated that the proposed rule should mandate that educational agencies provide parents with pre-printed forms, this mandate is beyond that required by §2 d, however, educational agencies may decide to provide these forms to parents.

81. COMMENT: Several commenters objected to the proposed rule as an unfunded mandate that will require additional funds be expended to meet the requirements of the proposed rule. One commenter asked if funding would be associated with the proposed rule. Another commenter stated that the statement in the regulatory impact statement that "The proposed amendment does not impose any direct costs on local governments beyond those imposed by the statute" is untrue. They further stated "…just as one example, the statute does not dictate the NIST CSF standards and districts, BOCES and vendors are not presently obligated to meet the requirements of those standards. There will most certainly be new costs imposed on educational agencies to meet the new NIST CSF standards if adopted. It is our

view that the regulatory impact statement filed with the proposed regulation is insufficient under State Administrative Procedure Act § 202-a, and request that a new impact statement be filed that meets the requirements of that law.

RESPONSE: The proposed rule is consistent with the requirements of Education Law §2-d. Education Law §2-d requires that the commissioner, in consultation with the Chief Privacy Officer, promulgate regulations that establish a standard for educational agency data security and privacy. The Department selected the NIST standard to implement the statutory requirements. The Department will revise its Regulatory Impact Statement to help clarify that due to the fact that the NIST standard is not a one size fits all standard and it has not been implemented in New York State, the Department does not have data that would enable to quantify an expected cost.

82. COMMENT: Several commenters requested that the Department issue a revised Armed Services Vocational Aptitude Battery (ASVAB) Directive for New York State following New York City's Rule A-825. This would require a parent and student to submit an opt-in form if they wish to have test data released.

RESPONSE: No change is necessary. The comment is beyond the scope of Education Law §2-d. However, the Department acknowledges these comments and will review them to determine if additional guidance is needed.

83. COMMENT: A comment was made about a copyrighted image the Department was purported to have used in a public presentation.

RESPONSE: The comment is unrelated to and outside the scope of the

rulemaking. As such, no response is necessary.

84. COMMENT: A commenter expressed concerns that the proposed rule “will impose significant legal liability upon school districts”. The commenter states the level of technical security school districts can provide in a cost-effective manner is almost certain to fail in the face of a sophisticated cyber-attack.
RESPONSE: The proposed rule implements Education Law §2-d. Therefore, no changes are necessary.

85. COMMENT: A commenter requested an extension of the public comment period so educational agencies may better understand the Rule.
RESPONSE: No change is necessary. The comment period complied with the provisions of the State Administrative Procedures Act (SAPA) §202(1)(a). Moreover, because the rule is being revised, an additional 45-day public comment period will be provided on the revised rule in accordance with SAPA.

86. COMMENT: Two commenters encouraged the Department to include all stakeholders, including third party providers, as part of the Data Privacy Advisory Council (DPAC).
RESPONSE: The DPAC included representation from a wide range of stakeholders including the Future of Privacy Forum, which is a nonprofit organization comprised of industry, academic, consumer advocate leaders to develop privacy protections, ethical norms and workable business practices. Moreover, this change is beyond the scope of the regulation. Therefore, no change is warranted.

87. COMMENT: A commenter expressed concern that the proposed rule was developed to limit the burden on school districts and school personnel rather than to protect Personally Identifiable Information.

RESPONSE: No change is necessary. The proposed rule implements Education Law §2-d and seeks to strengthen data security and privacy protections at educational agencies to safeguard personally identifiable information.

88. COMMENT: A commenter recommended that the proposed rule prohibit the deployment of biometric surveillance systems in educational agencies and address student biometric personally identifiable information as a separate category, rather than incorporating FERPA's definition, and requested that it expand on the FERPA definition of "biometric record" and set specific standards which establish that "biometric data" includes photos, videos, infrared scans, sound recordings, or other captured physical or behavioral characteristics of an individual, including but not limited to an individual's face, voice, fingerprint, appearance, and gait, that may be used to conduct face and biometric surveillance as well as any information derived from biometric information, including but not limited to assessments about an individual's sentiment, state of mind, or level of dangerousness." The commenter also stated the proposed rule should "prohibit any school district from obtaining, retaining, accessing, or using any student biometric information from any biometric surveillance system and prohibit the direct use of the biometric surveillance system by a law enforcement officer or law enforcement agency and any requests by a law enforcement officer that a law enforcement agency or other

third-party use the biometric surveillance system on behalf of the requesting entity."

RESPONSE: No change is necessary. The proposed rule adopts Education Law §2-d's definition of personally identifiable information which adopts FERPA's definition. FERPA defines personally identifiable information to include "students' social security number, student number or biometric record." Biometric records are further defined as "a record of one or more measurable biological or behavioral characteristics that can be used for automated recognition of an individual. Examples include fingerprints; retina and iris patterns; voiceprints; DNA sequence; facial characteristics; and handwriting" (34 CFR 99.3). The Department is aware of the concerns raised about the use of technology that utilizes biometric data in schools and continues to research and review these issues.

89. COMMENT: A commenter noted that a PowerPoint presentation by SED included the language that "the Department may withhold or claw back any related payments to an agency that is earmarked for the procurement of such technology or services where the agency is not in compliance with state and federal law and proposed rule." The commenter stated that this was outside the authority provided to the Chief Privacy Officer pursuant to Education Law §2-d.

RESPONSE: No change is necessary. The referenced language is outside the scope of the proposed rule.

90. COMMENT: A commenter stated that the Department should withdraw the proposed rule or substantially modify it to include substantially more protections of

student, principal and teacher personally identifiable information. The commenter believes that it does not go far enough in protecting personally identifiable information.

RESPONSE: No change is necessary. The proposed rule implements Education Law §2-d.

91. COMMENT: A commenter noted that compliance with the proposed rule may require the purchase of a system to manage data inventory, vendor privacy policy, and contract information. Another commenter noted that systems and programs that have access to personally identifiable information including networks and firewalls must be addressed by the proposed rule.

RESPONSE: No change is necessary. Education Law §2-d and the proposed rule requires educational agencies to adopt safeguards associated with industry standards and best practices including but not limited to encryption, firewalls, and password protection. The NIST Cybersecurity Framework outlines controls and provides guidance as to how these may be implemented. The Department will provide guidance, as needed, to assist educational agencies.

92. COMMENT: A commenter asked whether anonymizing student names is sufficient to address non-sharing of PII. The same commenter asked if “it would be allowed to aggregate student Regents scores on a particular test and share averages within three bands, or if we were to create a distribution of scores graph without PII.”

RESPONSE: Please see the definition of personally identifiable information in

Education Law §2-d and the proposed rule. As this comment asks questions that are beyond the scope of this rulemaking, no changes are necessary.

93. COMMENT: A commenter stated that it would be most helpful for NYSED to create
a clearinghouse of all vendors who meet the data privacy standards, rather than each district trying to discern this information on their own. Another commenter stated that “asking every single school district to have every vendor sign off on a contract including an addendum regarding how they are going to use student data is onerous to both the district and the vendors.” The commenter thought the process could be better administered at either the state level or with each of the RICs as “… it seems redundant for a vendor to have to sign off on 700+ individual contracts that state the exact same thing about what they do with student data.”
RESPONSE: Each educational agency is responsible for ensuring that their third party contracts are compliant with Education Law §2-d and the proposed rule. See response to Comment #43, which explains that the proposed rule does not prohibit school districts from seeking assistance and efficiencies through partnerships with third parties including BOCES, consistent with Education Law §1950.

94. COMMENT: A commenter stated that there was a lack of meaningful opportunities
for parents and guardians to be involved in the public comment sessions held by the Department.
RESPONSE: The Department held 14 public forums across the state, which

provided multiple opportunities for engagement with the public and stakeholders, and parents and guardians. These forums were held in the evenings with the goal of maximizing participation of parents and families. In addition, the Department worked with the Parent Teachers Association (PTA) to ensure the participation of parents in the forums.

95. COMMENT: A commenter asked whether “extensions such as Google Chrome count as separate vendors or as third-party vendors via Google?”
RESPONSE: Please refer to the definition of third-party contractor in Education Law §2-d and the proposed rule.

96. COMMENT: A DPAC member commented about the limited number of opportunities for DPAC members to engage in further dialogue beyond the meetings where members had the opportunity to discuss their concerns with the proposed rule. The commenter also stated that the Department did not distribute the emailed comments of other members amongst all DPAC members, and that not all members of the DPAC participated in the sub-committee that drafted the proposed rule and believed that this resulted in the perspectives of advocates for student privacy being left out. The same commenter also expressed disappointment that discussions at a DPAC meeting focused on “the goal of ensuring a limited burden on school districts and school personnel with respect to the implementation of 2-d – rather than ensuring protection of student, and staff, Personally Identifiable Information and balancing the efforts to do so against any burdens imposed on school districts and school personnel.”

RESPONSE: DPAC members were drawn from a broad selection of stakeholders to ensure input was both deep and diverse. It was inefficient to have every member participate on the drafting committee which consisted of 5 non-Department staff members. However, the input of all DPAC members was carefully considered and incorporated where possible.

97. COMMENT: A commenter asked if the dollars expended on this effort would be exempt from the Tax Cap?

RESPONSE: This comment falls outside the scope of the proposed rule.

98. COMMENT: A commenter asked if the Department had any suggestions for how to

handle software orders for the 2019-20 school year, especially considering that the agency purchases multi-year licenses to take advantage of discounts and they may not know if a vendor will comply with the law's requirements.

RESPONSE: Each educational agency is responsible for ensuring that their third party contracts are compliant with Education Law §2-d and the proposed rule. The Department will provide guidance, as needed, to assist educational agencies.

99. COMMENT: A commenter stated that many schools have successfully integrated

GSuite for teaching and learning, which is a major investment, and asked when we will know if Google will sign the requisite documents to be in compliance.

RESPONSE: Each educational agency is responsible for ensuring that their third

party contracts are compliant with Education Law §2-d and the proposed rule.

100. COMMENT: A commenter appeared to suggest that educational agencies should be permitted to accept the online terms of service of third-party contractors in lieu of a negotiated contract that complies with Education law §2-d. The comment read “It should be the expectation of the school district to read and understand the third party contractor privacy disclosure balancing that with instructional implications. There should not be a need to send for example, Google, a document with this information. Can our voice be heard by a large corporation like Google? We agree with their privacy statement. Can that be enough? Publishing it on the district website is feasible, but sending the document is not for many products used. In other words, the district should be aware and have read the privacy statement for the product and agree to it, or not use it.”

RESPONSE: Clickwrap agreements that include third-party contractors’ terms of service and other terms and conditions are “contracts and other written agreements” that must comply with the requirements of the statute and proposed rule. Therefore, no change to the proposed rule is warranted.