Strengthening Data Security and Privacy in NYS Educational Agencies

Discussing the Proposed Part 121 of the Regulations of the Commissioner of the NYS Education Department

Tope Akinyemi,
Chief Privacy Officer, NYSED

NYS ED .gov New York State EDUCATION DEPARTMENT Knowledge › Skill › Opportunity

PROPOSED PART 121 - UPDATE

- Published January 31st in the State Register
- Public comment period open for 60 days till April 1
- SED will analyze received comments and revise rule, as applicable
- If substantive revisions are made, SED must submit a Notice of Revised Rule Making to open another 30 day comment period before adoption
- If no material revisions are needed, rule will be presented to the Regents for adoption, possibly on May 6th
- If adopted, it becomes effective July 31st
- SED will continue to work with workgroup and stakeholders to develop resources for implementation

Public Comment - Summary of Issues

ISSUE	RESPONSE
Whether Ed Law §2-d and Part 121 apply to charter schools as charter schools are expressly included in the definition of schools in proposed Part 121.	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. The Department's position is that Education Law §2-d and the proposed rule apply to charter schools.
Impact of Part 121 on the use of software applications with non-compliant clickwrap agreements on technology based classroom learning.	The statute applies regardless of the form of contract utilized. Making an exception merely based on the form of contracting would not align with the purpose of the statute to protect personally identifiable information.
Concerns about whether Part 121 would preclude entities that offer college entrance examinations from providing student data to colleges.	We added a provision that where a parent/eligible student requests a service or product from a third-party contractor and provides express consent to the use or disclosure of PII by the 3rd party contractor for purposes of providing the requested product or service, such use shall not be deemed a marketing or commercial purpose prohibited by the proposed rule.

Public Comment – Summary of Issues (contd.)

ISSUE	RESPONSE
Concerns about funding and costs.	Proposed Part 121 is consistent with the requirements of Education Law §2-d and does not impose costs beyond that imposed by the statute.
Aggressive timeline concerns.	Proposed Part 121 included only one date – the date educational agency’s must adopt the Data Privacy and Security Policy. The original date was December 1, 2019 but is now July 1, 2020.
Whether the NIST Framework is applicable to the education sector, and whether it is robust enough to protect student data.	The NIST Cybersecurity Framework is a national standard that is also flexible to allow entities to implement it from a risk based approach, and is intended to be tailored to different sectors such as the education sector.
Questions about the Data Protection Officer’s role, finding qualified personnel and whether a shared services model could be applied.	SED does not believe that an educational agency can completely outsource the job function of a Data Protection Officer but does not prohibit the use of a 3rd party such as a BOCES from providing some of the functions.
Request that professional service providers (e.g. school attorneys, school physicians, school psychologists, etc.) rules of ethics and practice be allowed as a substitute for compliance with	SED does not believe that such rules are equivalent substitutes for the data security and privacy requirements for protecting PII. Such an exception is not contemplated by the law and permitting it could jeopardize the privacy and security of PII and very sensitive data that

Public Comment – Summary of Issues (contd.)

ISSUE	RESPONSE
Armed Services Vocational Aptitude Battery Test (ASVAB) related comments that Part 121 does not do enough to protect student PII from military recruiters.	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.
Requests that SED (or BOCES in the alternative) negotiate state contracts for districts, maintain an approved list of compliant/approved vendors (clearinghouse).	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.

Review of Proposed Part 121 Revisions

121.1	Definitions
	Added a definition of encryption
	Clarified that parents and eligible students may sign up for services and consent to the use of PII that they provide to a vendor
	Revised the definition of ‘commercial and marketing purpose’ to replace ‘profit’ with ‘remuneration’
121.2	**Educational Agency Data Collection Transparency and Restrictions**
	Revised to incorporate provisions from Ed. Law §2-d
121.3	**Parent’s Bill of Rights**
	Revised to incorporate provisions from Ed. Law §2-d

Review of Proposed Part 121 Revisions (contd.)

121.4	Parent Complaints of Breach or Unauthorized Release of PII
	Revision made to permit agencies to require that complaints must be made in writing
121.5	NIST Cybersecurity Framework
	Revision made to provide that agencies must now complete and post their Data Privacy and Security Policies by July 1, 2020 instead of December 1, 2019
121.6	Data Security and Privacy Plan
	No change
121.7	Training for Educational Agency Employees
	Revision made to add examples of the types of training that could be provided

Review of Proposed Part 121 Revisions (3)

121.8	**Data Protection Officer**
	No change
121.9	**Third Party Contractors**
	Revised for clarity
121.10	**Reports and Notifications of Breach and Unauthorized Release**
	No change
121.11	**Third Party Contractor Civil Penalties**
	Revised to incorporate provisions from Ed. Law §2-d
121.12	**Right of Parents and Eligible Students to Inspect and Review Student Education Records**
	No change
121.13	**The Powers of the Chief Privacy Officer**
	Revised to incorporate provisions from Ed. Law §2-d

THE NIST CYBERSECURITY FRAMEWORK

Part 121 adopts the NIST Cybersecurity Framework as the standard for educational agencies data security and privacy policies and programs. Goals are to:

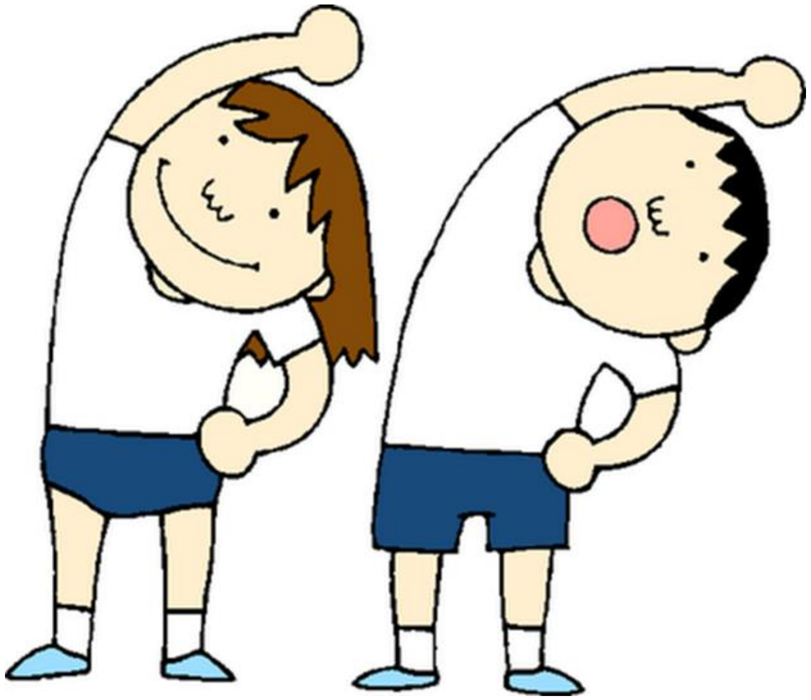
- Protect PII
- Strengthen cybersecurity programs in NYS educational agencies
- Reduce cybersecurity risk
- Use common language/consistent, standard controls
- Produce data to aid assessment of program effectiveness and maturity

NIST FRAMEWORK …

"The Framework enables organizations – regardless of size, degree of cybersecurity risk, or cybersecurity sophistication – to apply the principles and best practices of risk management to improving security and resilience."

NIST Framework for Improving Critical Infrastructure Cybersecurity, v1.1, Barrett et al, April 16, 2018, page v, Executive Summary
https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf

… A STANDARD WITH FLEXIBILITY



"The Framework is adaptive to provide a flexible and risk-based implementation."

Steps towards implementing the Framework

- NIST recommends that organizations follow a seven step risk management process
- SED and its Implementation Workgroup are reviewing ways to streamline the process and develop templates for districts
- SED will provide a roadmap and resources to aid implementation planning.

Step 1: Prioritize and Scope

CSF Documentation

The organization identifies its business/mission objectives and high-level organizational priorities, the organization makes strategic decisions regarding cybersecurity implementations and determines the scope of systems and assets that support the selected business line or process.

Support

- SED will provide MODEL TEMPLATES to assist with this step.

Step 2: Orient

CSF Documentation

Once the scope of the cybersecurity program has been determined for the business line or process, the organization identifies related systems and assets, regulatory requirements, and overall risk approach. The organization then consults sources to identify threats and vulnerabilities applicable to those systems and assets.

Support

SED will provide/facilitate:

- Inventory templates and tools
- Generic threat profile
- Connections to State agency resources for on-going expert information identifying threats and the need for new protections (e.g. NYS Office of Information Technology Services, Cybersecurity Advisories).

Step 3: Create a Current Profile

CSF Documentation

The organization develops a Current Profile by indicating which Category and Subcategory outcomes from the Framework Core are currently being achieved. If an outcome is partially achieved, noting this fact will help support subsequent steps by providing baseline information.

Support

- SED will work with implementation workgroup to identify a web-based tool to assess the level of protection currently achieved by the district (e.g. NCSR).

Step 4: Conduct a Risk Assessment

CSF Documentation

The organization analyzes the operational environment in order to discern the likelihood of a cybersecurity event and the impact that the event could have on the organization. It is important that organizations identify emerging risks and use cyber threat information from internal and external sources to gain a better understanding of the likelihood and impact of cybersecurity events

Support

- SED will facilitate connections to State agency resources for on-going expert information identifying threats and the need for new protections (e.g. NYS Office of Information Technology Services, Cybersecurity Advisories
- SED will provide model templates/resources to aid this step

Step 5: Create a Target Profile

CSD Documentation

The organization creates a Target Profile that focuses on the assessment of the Framework Categories and Subcategories describing the organization's desired cybersecurity outcomes. Organizations also may develop their own additional Categories and Subcategories to account for unique organizational risks. The organization may also consider influences and requirements of external stakeholders such as sector entities, customers, and business partners when creating a Target Profile. The Target Profile should appropriately reflect criteria within the target Implementation Tier.

Support

- SED will provide a model Target Profile

Step 6: Determine, Analyze, and Prioritize Gaps

CSF Documentation

The organization compares the Current Profile and the Target Profile to determine gaps. Next, it creates a <u>prioritized action plan to address gaps</u> – reflecting mission drivers, costs and benefits, and risks – to achieve the outcomes in the Target Profile. The organization then <u>determines resources</u>, including funding and workforce, necessary to address the gaps. Using Profiles in this manner encourages the organization to make informed decisions about cybersecurity activities, supports risk management, and <u>enables the organization to perform cost-effective, targeted improvements</u>.

v3/JF

Support

- Districts will be provided guidance

Step 7: Implement Action Plan

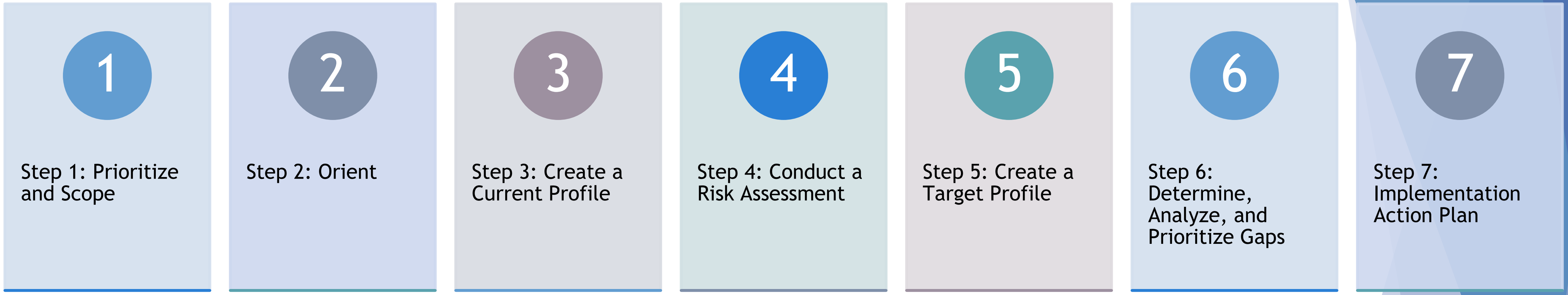
CSF Documentation

The organization determines which actions to take to address the gaps, if any, identified in the previous step and then adjusts its current cybersecurity practices in order to achieve the Target Profile. For further guidance, the Framework identifies example Informative References regarding the Categories and Subcategories, but organizations should determine which standards, guidelines, and practices, including those that are sector specific, work best for their needs.

Support

- Districts will be provided with sample/model plans to aid this process.

NIST Framework 7-Step Process



1. Step 1: Prioritize and Scope
2. Step 2: Orient
3. Step 3: Create a Current Profile
4. Step 4: Conduct a Risk Assessment
5. Step 5: Create a Target Profile
6. Step 6: Determine, Analyze, and Prioritize Gaps
7. Step 7: Implementation Action Plan

SED will support implementation

SED will provide support with some or all of the following:

- Resources
- Templates and model forms
- Technical expertise
- Implementation workgroup support
- Training and workshops

QUESTIONS AND DISCUSSION

Thank you.

Tope Akinyemi

Chief Privacy Officer, NYSED

Temitope.Akinyemi@nysed.gov