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

at the NASTECH Long Island Technical Directors Meeting

April 11, 2019

Tope Akinyemi,
Chief Privacy Officer, NYSED

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

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:

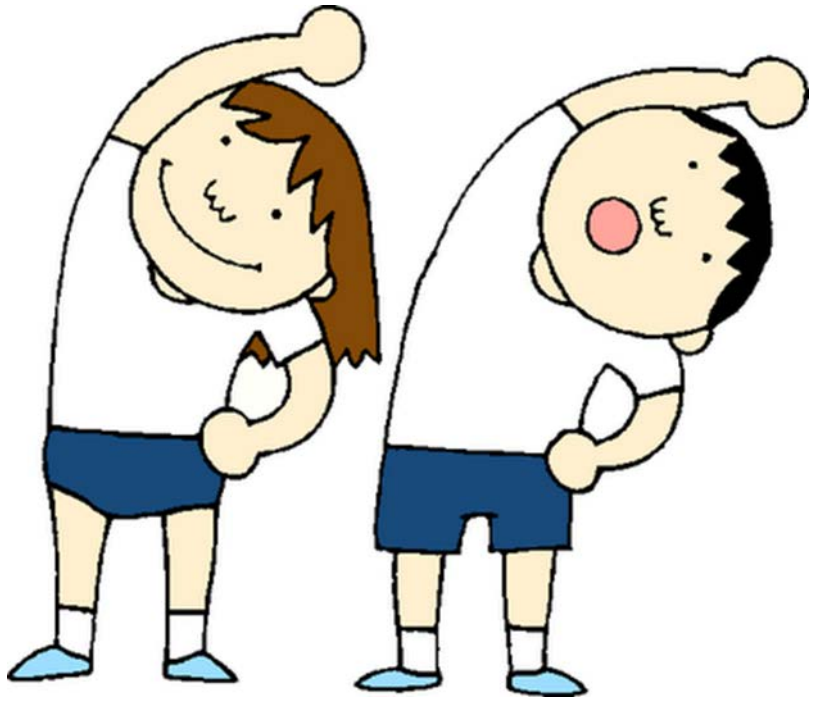
- Protect PII
- Strengthen cybersecurity programs in NYS educational agencies
- Reduce cybersecurity risk
- Use common language/consistent, standard controls
- Produce data to aid assessment of program effectiveness and maturity

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."

Benefits of the Framework compared to other standards

- Flexible implementation
- Focus is not on checklist - compliance is less about adhering to a list of To Dos and more about adhering to an established, ongoing, repeatable process
- Progress can be one measure of compliance
- Focus is on data security and privacy risk management

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 prioritized action plan to address gaps – reflecting mission drivers, costs and benefits, and risks – to achieve the outcomes in the Target Profile. The organization then determines resources, 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 enables the organization to perform cost-effective, targeted improvements.

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.

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