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

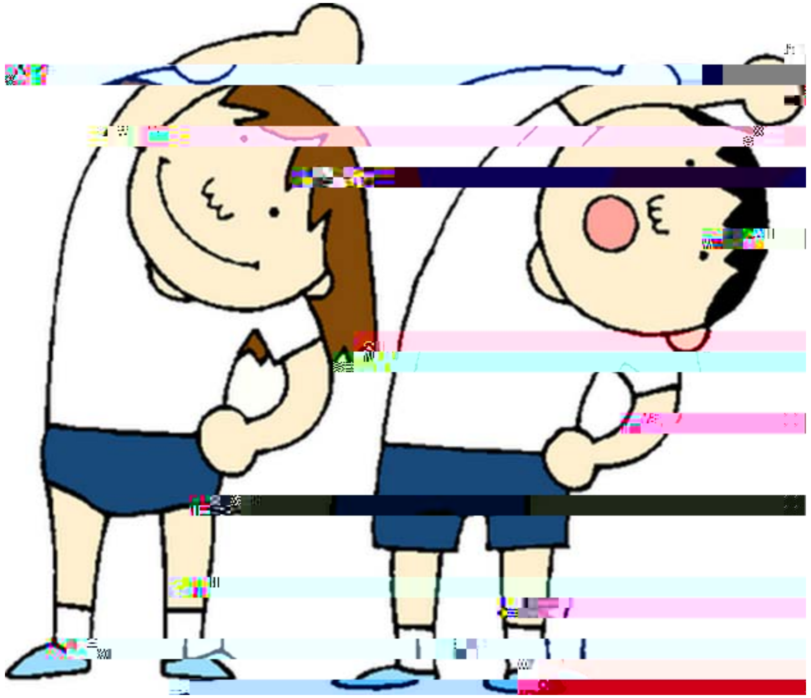
If no material revisions are needed, rule will be presented to the Regents for adoption, possibly on May 6th

If adopted, it becomes effective July 31st

SED will continue to work with workgroup and stakeholders to develop resources for implementation

NIST FRAMEWORK …

… 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 a-540 l 98.293 0 l httd03

Steps towards implementing the Framework

NIST recommends that organizations follow a seven step risk management process

SED and its Implementation Workgroup are reviewing ways

Step 1: Prioritize and Scope

CSF Documentation

The organization identifies its business/mission objectives and high-level organizational priorities

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 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

QUESTIONS AND DISCUSSION

Thank you.

Tope Akinyemi

Chief Privacy Officer, NYSED