New York State
EDUCATION DEPARTMENT
Knowledge › Skill › Opportunity

Student Data Privacy Updates

MAY 7, 2018

Draft Regulations

Regulations will:

- Implement the statute's provisions.
- Supplement the parent's bill of rights for data privacy and security.
- Clarify uncertainties.
- Establish information security and privacy standards.
- Inform model policies.

2-d (5)(b) - The standards for data security and privacy policies shall include:

Data privacy protections.

Criteria to ensure that the use of PII benefits students and educational agencies.

Processes to ensure that PII is not included in public reports or other public documents.

Data security protections for data systems monitoring, data encryption, incident response plans, limitations on access and safeguards for PII transmittal over communication networks, and destruction of PII when no longer needed.

Application of the standards to third-party contractors.

Options Considered

Home grown standard

Patchwork of homegrown, private and national standards

National standard

Consulted with:

- The Data Privacy Advisory Council (DPAC)
- Public and Private Sector Technical Experts
- US Department of Education
- Other States

Preferred Qualities for a Standard

Credible (established by consensus, approved by a recognized body)

Durable (stands the test of time)

Enforceable (can be audited, if needed)

Understandable (relatable)

Supportable (provides for common guidelines for repeated use and consistent application)

Proposing NIST 800-171

- The National Institute of Standards and Technology 800-171 standard addresses the confidentiality and privacy of confidential information
- Meets the above noted qualities:
  - Credible - most other standards are derived from NIST standards.
  - Durable - US Department of Commerce keeps the standard current.
  - Enforceable - audit resources exist for NIST standards.
  - Understandable - most widely adopted data privacy and security standard in the United States.
  - Supportable - knowledge transfer to districts and vendors supported by federal and private sector resources.

Other Standards Considered

- The Consortium for School Networking, COSN
- Center for Internet Security, CIS
- NYS Enterprise Information Security Office
- US Department of Education's Privacy Technical Assistance Center
- Electronic Privacy Information Center, EPIC.org
- FedRAMP (applies NIST to Cloud providers)
- NYS Comptroller Best Practices

Benefits of Adopting a Standard

Helps establish common security requirements.

Helps better understand, manage, and reduce cybersecurity risks.

Helps prioritize investments and maximize the impact of each dollar spent on cybersecurity.

Used as a strategic planning tool to assess risks and current practices.

Incorporates best practices and conformance requirements.

Reduces the number of technical and process variations.

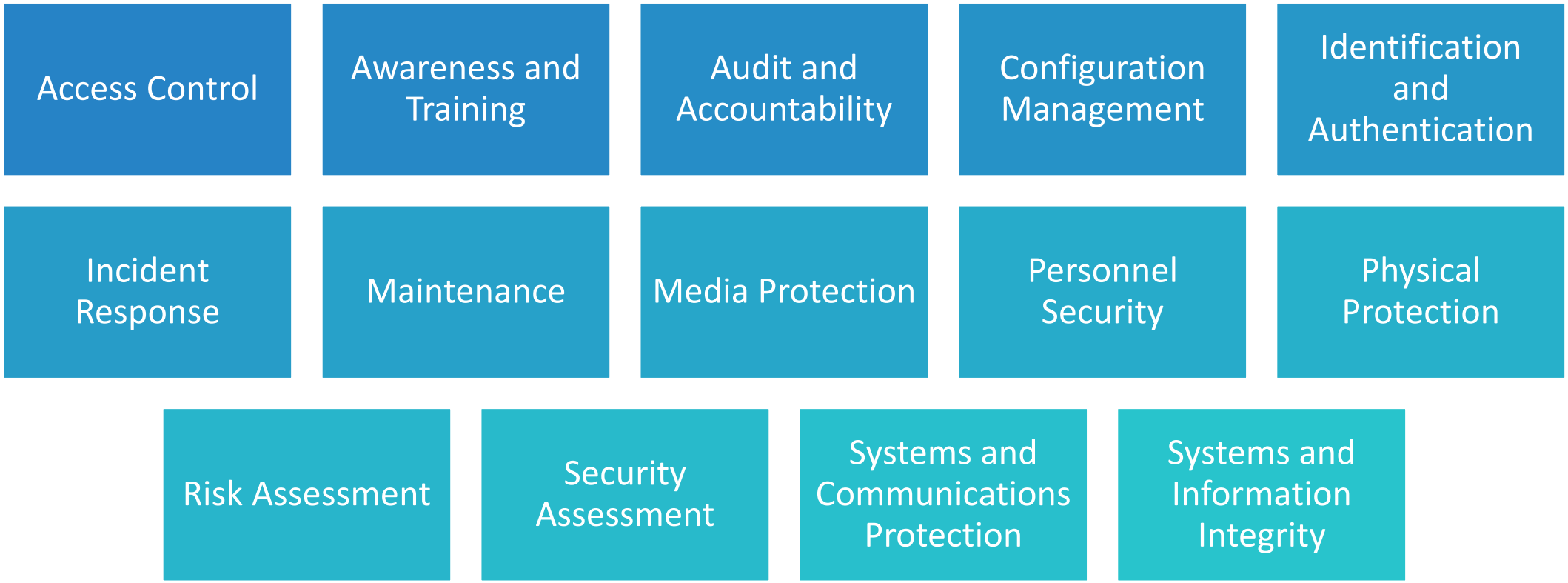
Offers a way to measure products and services against objective criteria and provide a basis for comparing products.

Implements security controls that meet legal and regulatory requirements.

National Institute of Standards and Technology (NIST)

- NIST is a federal agency within the United States Department of Commerce whose mission is to develop and promote measurement, and standards.
- NIST is also responsible for establishing computer and information technology related standards and guidelines for federal agencies to use.
- Many private sector organizations have made widespread use of these standards and guidelines voluntarily for several decades.

NIST 800-171 consists of 14 Families of Security Requirements

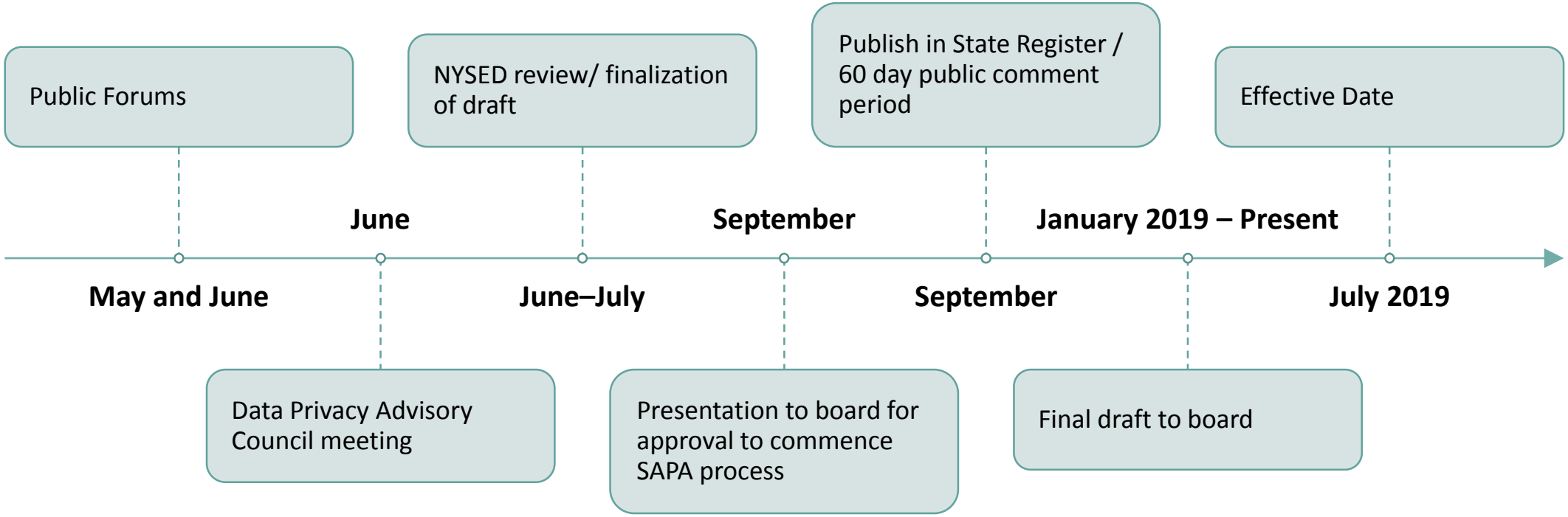


Tailoring the standard to NYS K-12

NIST 800-171 can be tailored to align the controls with the specific concerns/needs of stakeholders as part of a tailoring process which can include:

- Identifying and designating common controls;
- Applying scoping considerations;
- Selecting compensating controls;
- Assigning values to organization-defined control parameters via explicit assignment and selection statements;
- Supplementing baselines with additional controls and control enhancements; and
- Providing specification information for control implementation.
- Tailoring must be defensible based on mission and business needs, a sound rationale, and explicit risk-based determinations.

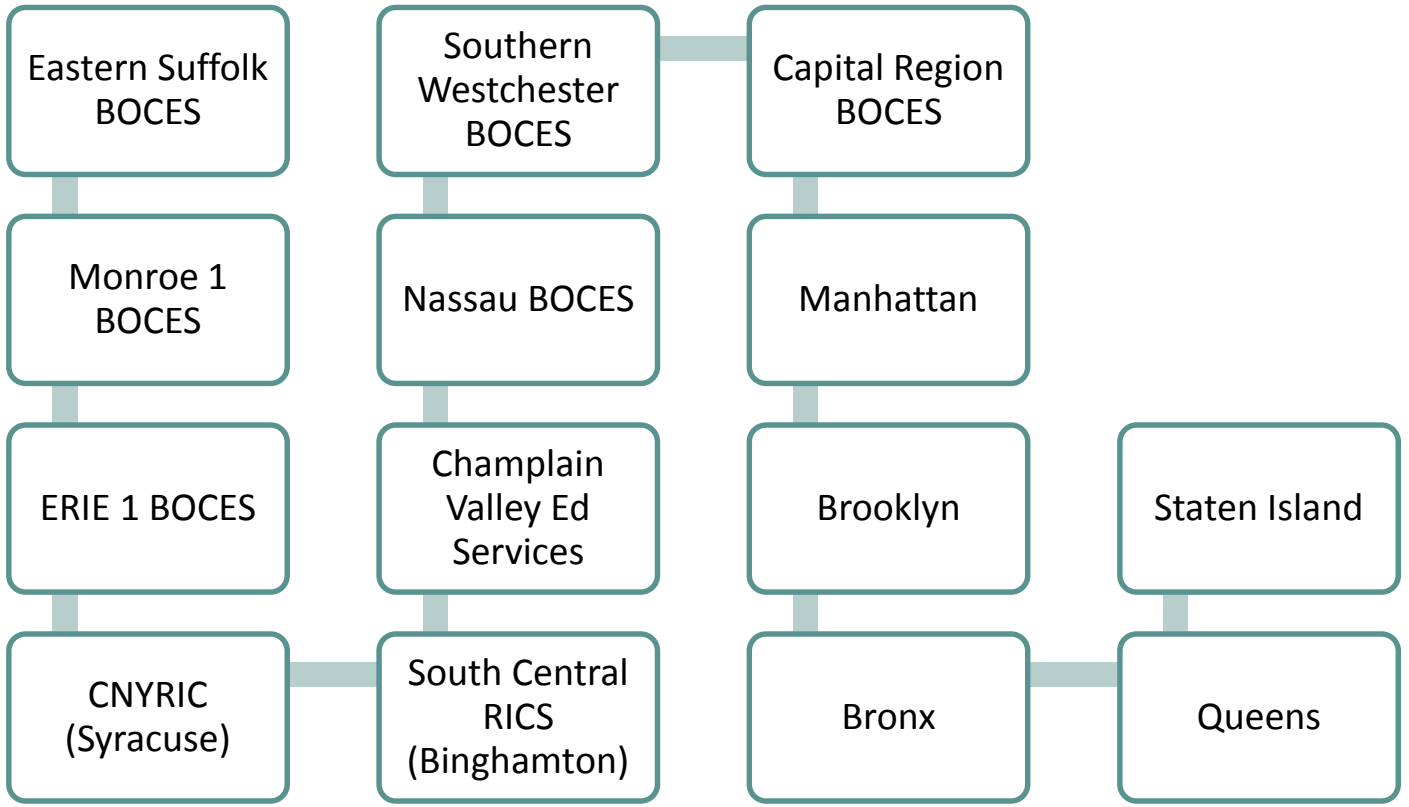
Regulatory Proposal Timeline



Data Collection Transparency

- Reviewed collection practices and eliminated 3 data elements:
  - Date of Entry into the United States
  - Country of origin
  - Immunization Date for First Polio Vaccination
- Added one new data element pursuant to NYS's approved ESSA plan:
  - Out-of-school suspensions data (Beginning in the 2017-18 school year New York State started collecting out-of-school suspensions data at the individual student level to aid with holding schools accountable for out-of-school suspension rates as a measure of school quality and student success.)
- The data elements table on NYSED's website will be updated with this new information.

Planned Public Forums – May 1-11 and June 4-15, 2018



Purpose of Forums

Get input from parents, education and expert stakeholders to develop additional elements of the parents bill of rights for data privacy and security.

Get feedback about the privacy and security of PII.

Gain a better understanding of provider experiences (teachers, administrators, etc.).

Not a substitute for SAPA 60 day comment period that will commence in the Fall.

Each forum is two hours long, from 6- 8 p.m., with every registered participant allocated a maximum of three minutes to provide input.

Comments can also be submitted online to *privacycomment@nysed.gov*.

Some Partners in the Work:

Data Privacy Advisory Council (DPAC)

DPAC Work Group Members

- Heather Mahoney -
- Colleen Sloan
- Joseph Baranello
- Joseph Fitzgerald
- David Pellow

- Michelle Okal-Frink
- Patrick McGrath
- Tracy Falvo

Questions and Discussion.

Thank you.