New York State
EDUCATION DEPARTMENT

Knowledge › Skill › Opportunity

January 14, 2019

Proposing Part 121 of Commissioner's Regulations – Protecting PII in Educational Agencies (Education Law 2-d Regulations)

Presentation Agenda

- Review of Proposed Rule by Section
- National Institute of Standards and Technology Cybersecurity Framework (NIST CSF)
- Implementation Resources
- Timeline

Stakeholder Participation

Data Privacy Advisory Council comprised of varying stakeholders (parent advocates, teacher and administrative organizations, district officials and technical experts)

Technical Standard Workgroup comprised of information technology and security experts

14 Public Forums held statewide to receive public comment - attended by parents, advocate groups, teachers and teachers' unions

Input received from industry groups and public sector representatives related to additional elements of the parent’s bill of rights

Implementation Work Group (RIC Directors, BOCES District Superintendents and staff, School Technology Directors)

Part 121 - 2-d – Index of Sections

121.1- Definitions

Commercial or Marketing Purpose	Contract or other written agreement
Sale of student data or its use or disclosure, whether directly or indirectly to derive a profit, for advertising purposes or to develop, improve or market products or services to students.	Includes agreements in electronic form, signed with an electronic or digital signature, or a click wrap agreement.

121.2 Educational Agency Data Collection Transparency and Restrictions

Educational Agencies cannot sell or disclose PII for any marketing or commercial purpose.

Educational Agencies must take steps to minimize the collection, processing and transmission of PII.

Educational Agencies must manage contractual relationships to ensure compliance with laws and regulations.

Educational Agencies must manage clickthrough agreements for online or downloaded applications which use PII.

121.3 Parent's Bill of Rights

Must be published on educational agency's website

Must be included in each contract where PII will be provided and include supplemental information about the contract and third-party contractor's data protection practices

Must publish supplemental contract information or substantial equivalent

121.4 Parent Complaints of Breach or Unauthorized Release of PII

Procedure

- EAs must establish a procedure for parents and eligible students to file complaints about breaches or unauthorized releases of student data.

Communication

- …and must acknowledge receipt of complaint, investigation and precautions to protect PII.

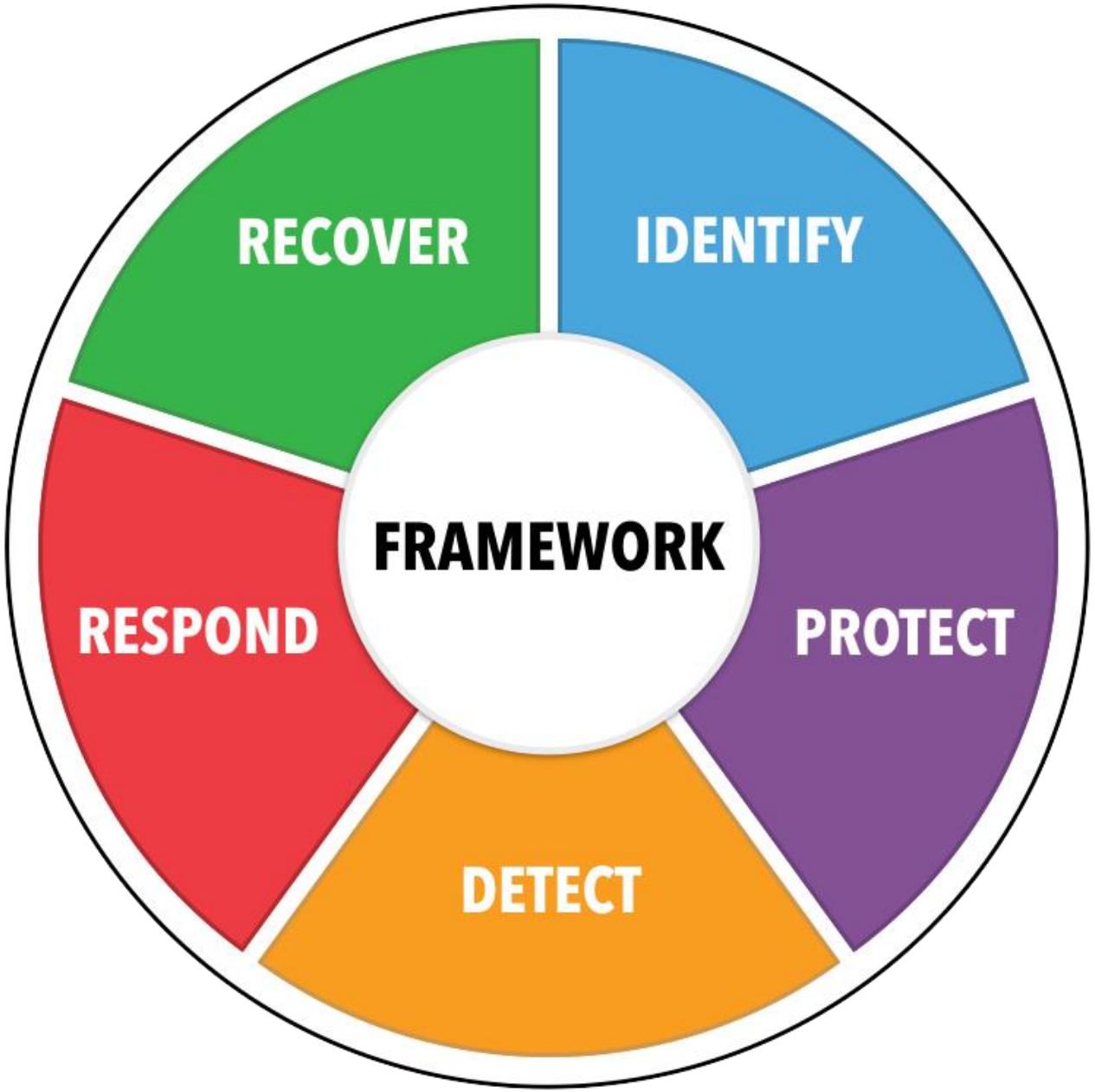
Investigate and Notify

- …and must provide a report of findings within 30 days unless there is an extenuating circumstance.

Record Keeping

- … and maintain a record of all complaints and their disposition.

121.5 NIST CSF (National Institute of Standards and Technology Cybersecurity Framework) is the Data Security and Privacy Standard for Educational Agencies



121.6 Data Security and Privacy Plan

Required for every third-party contract that will utilize PII to detail data protection structure and practices, and plan to comply with laws and regulations.

Officers or employees of contractor who access PII receive training on all applicable laws governing confidentiality prior to receiving access.

121.7 Training for Educational Agency Employees

Educational Agencies must annually provide information privacy and security awareness training to their officers and employees with access to PII.

Online training tools may be used to provide this training. Data Security and Privacy training may be included as part of other training offered to employees.

121.8 Data Protection Officer

Each educational agency must designate one or more employees with appropriate knowledge, training and experience to serve as the data protection officer.

May be filled by a current employee.

Will be responsible for the implementation of the policies and procedures required under Education Law §2-d and the regulations.

Will be point of contact for data security and privacy for the educational agency.

121.9 Third Party Contractors

Must comply with NIST standard, Policy, Plan, laws and regulations

Must not disclose PII to any third party/must limit access.

Must only use PII for authorized contract purposes

Must not sell PII.

121.10 Reports and Notifications of Breach and Unauthorized Release

Third Party Contractors must notify EAs within 7 days of discovery of a breach/unauthorized release. Where the breach is attributable to a third-party contractor, the contractor will reimburse the educational agency for notification costs.

Educational Agencies must report breaches of PII to the Department's CPO within 10 calendar days; and must notify affected parents/eligible students/teachers/or principals within 14 days of discovery (later under certain circumstances).

121.11 Third Party Contractor Civil Penalties

The statute permits the CPO to impose civil penalties

Regulations address investigations of breaches/ unauthorized releases of PII

CPO may require parties to:

- Submit documentation
- Provide testimony
- Examination and inspection of facilities and record
- Provide a written response

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

Includes a process for parents and eligible students to exercise their right to inspect and review education records.

Access should be provided within 45 calendar days.

Educational agencies will ensure only authorized individuals access student data.

Educational agencies must notify parents annually of this right. A notice issued by the agency to comply with FERPA will satisfy this requirement.

121.13 The Powers of the Chief Privacy Officer

To execute the duties of Education Law §2-d, the CPO has the power to access all records, reports, audits, reviews, documents, papers, recommendations and other materials that relate to PII, and to comment on any Department program, proposal, grant or contract that involves PII.

The CPO may require educational agencies to perform privacy and security risk assessments to ensure the protection of PII where the agency seeks to procure a technology product or service that stores PII.

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 regulations.

Education Law 2-d requirements for a standard:

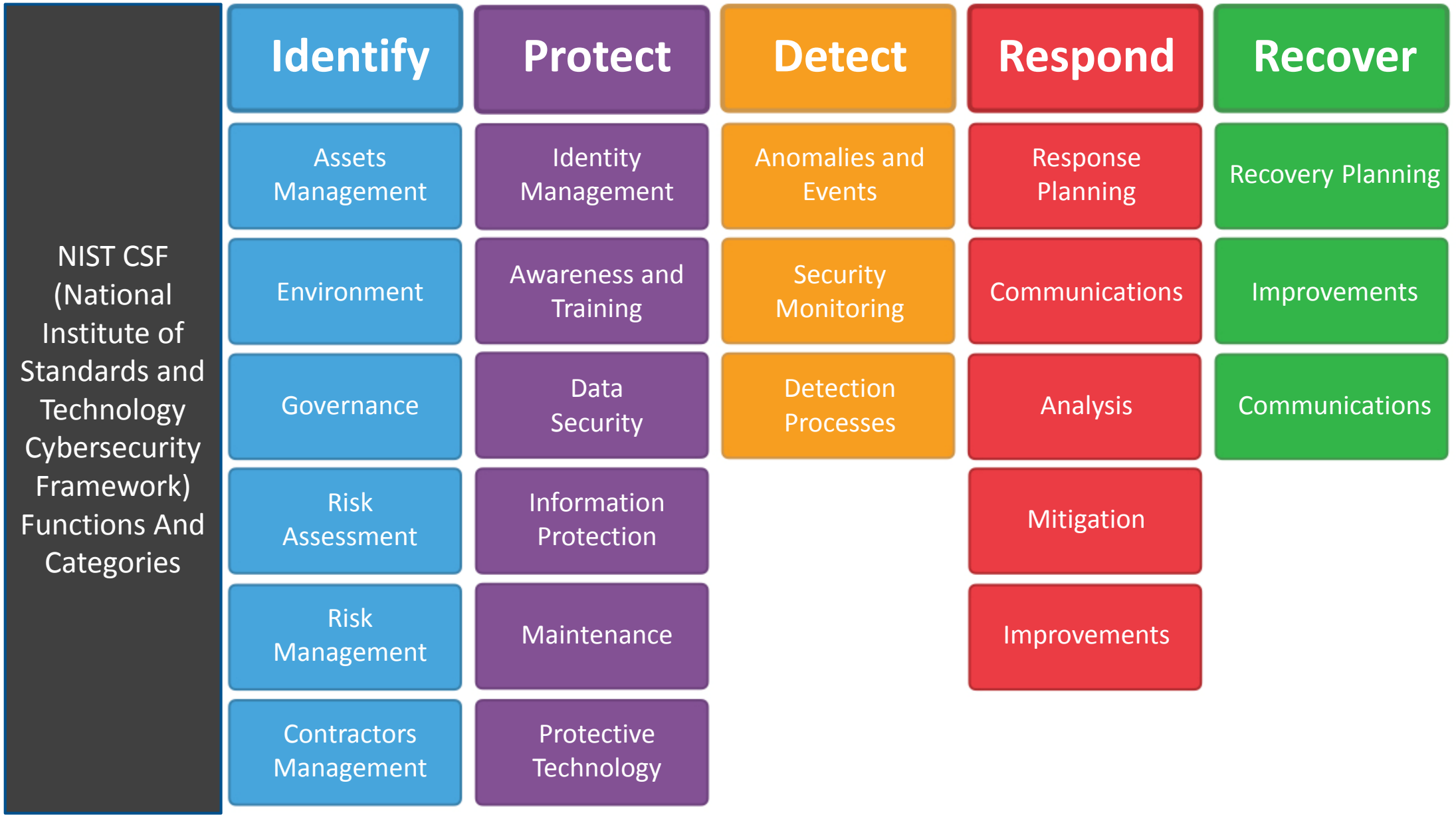
- Data privacy protections.
- Criteria to ensure that the use of PII benefits students and educational agencies.
- Processes to ensure that PII is not included in public reports or other public documents.
- Protections for data systems monitoring, data encryption, incident response plans, limitations on access, safeguards for PII transmittal, and destruction of PII.
- Application of the standards to third-party contractors.

NIST CSF (National Institute of Standards and Technology Cybersecurity Framework)

NIST is a federal agency within the United States Department of Commerce. whose mission is to develop and promote measurement, standards, and technology to enhance productivity, facilitate trade, and improve the quality of life.

NIST CSF consists of standards, guidelines, and best practices to manage cybersecurity-related risk, establish a data security and privacy program.

The NIST CSF Core is a set of specific activities to manage data security and privacy risk organized into 5 functions, 23 categories, and 108 subcategories.

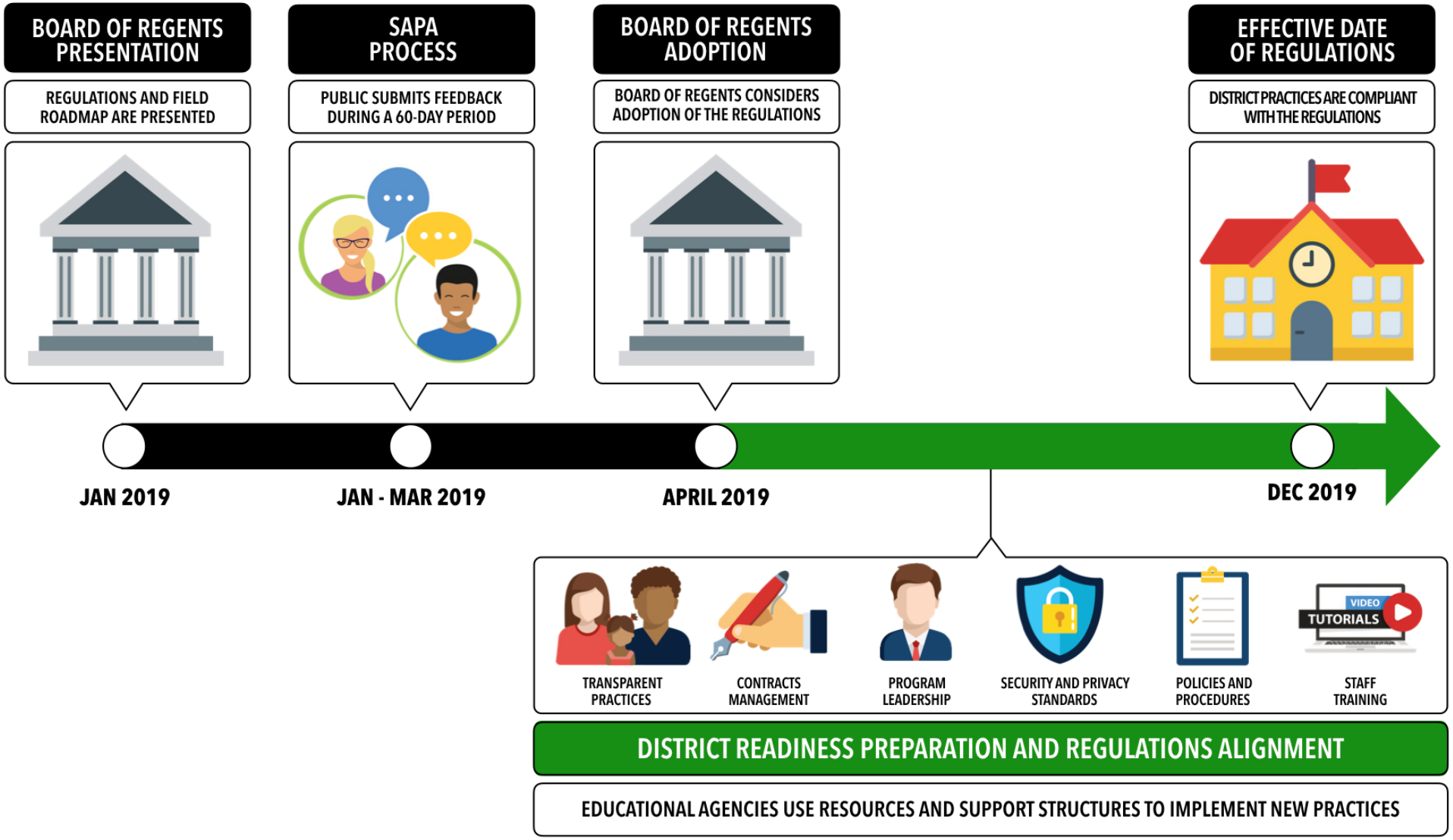

NIST CSF (National Institute of Standards and Technology Cybersecurity Framework) Functions And Categories
Identify
Assets Management
Environment
Governance
Risk Assessment
Risk Management
Contractors Management
Protect
Identity Management
Awareness and Training
Data Security
Information Protection
Maintenance
Protective Technology
Detect
Anomalies and Events
Security Monitoring
Detection Processes
Respond
Response Planning
Communications
Analysis
Mitigation
Improvements
Recover
Recovery Planning
Improvements
Communications

Implementation Resources

Collaborating with NYS ITS, BOCES and RICs to develop resources:

- Educational materials and guidance literature
- Model Data Security and Privacy Policy
- Data Security and Privacy Contract Addendum/Model terms and conditions
- Tools for NIST CSF gap analysis

Implementation Timeline



Discussion.

Thank you.