



CYBERSECURITY TIPS AND TOOLS - SB 820 AND HB 3834 (86TH) UPDATES FOR TEXAS SCHOOL DISTRICTS

Frosty Walker

Chief Information Security Officer

Texas Education Agency

Frosty.Walker@tea.texas.gov

(512) 463-5095



Data Security Advisory Committee

The Data Security Advisory Committee (DSAC) provides guidance to the Texas education communities, maximizing collaboration and communication regarding information security issues and resources which can be utilized within the educational communities served.

The DSAC is currently comprised of representatives from school districts, ESCs, TEA and the private sector.

Texas Gateway

<https://www.texasgateway.org/>

Cybersecurity Tips and Tools

A decorative graphic consisting of several parallel white lines of varying lengths, slanted diagonally from the bottom right towards the top right, located in the lower right quadrant of the slide.



Online resources
FOR YOUR CLASSROOM

Find engaging, TEKS-aligned resources that you can use with your students as part of classroom instruction, intervention, acceleration, or additional practice.

show me more











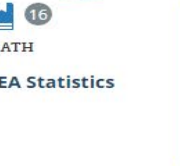

BROWSE TEKS

BROWSE RESOURCES

Search

Featured Resources

1 of 2

 <p>EARLY CHILDHOOD Prekindergarten Enrollment Toolkit</p>	 <p>MATH ESTAR/MSTAR</p>	 <p>Open-Source Instructional Materials</p>	 <p>openstax STUDY EDGE</p>	 <p>Cybersecurity Tips and Tools</p>	 <p>Restorative Discipline Practices in Texas</p>
 <p>ELA & READING Complete "Red Book Series" Focused on Reading Instruction</p>	 <p>TEXAS LESSON STUDY Texas Lesson Study Briefing</p>	 <p>Starting the Conversation</p>	 <p>MATH TEA Statistics</p>	 <p>Statistics</p>	 <p>Statistics</p>

SB 820

(b) Each school district shall adopt a cybersecurity policy to:

- (1) Secure district cyberinfrastructure against cyber-attacks and other cybersecurity incidents
- (2) Determine cybersecurity risk and implement mitigation planning
- (3) Designate a Cybersecurity Coordinator
- (4) Report a “breach of system security” to TEA
- (5) Notify parents of breach of protected student information

(c) School district’s cybersecurity policy may not conflict with the information security standards for institutions of higher education adopted by the Department of Information Resources under Chapters 2054 and 2059, Government Code. (**Texas Cybersecurity Framework**)

SB 820

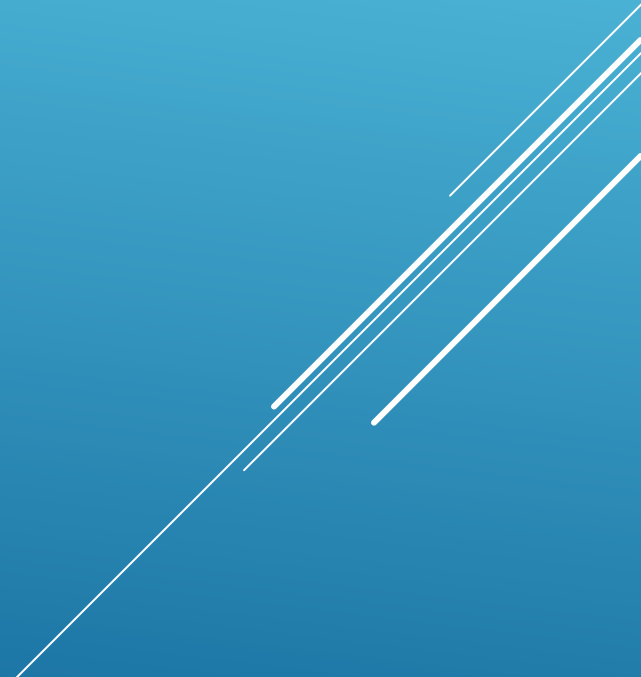
(d) The superintendent of each school district shall designate a cybersecurity coordinator to serve as a liaison between the district and the agency in cybersecurity matters. (in the AskTED application)

(e) The district 's cybersecurity coordinator shall report to the agency any cyber-attack or other cybersecurity incident against the district cyberinfrastructure that constitutes a **breach of system security** as soon as practicable after the discovery of the attack or incident.

(1) “ **Breach of system security**” means an incident in which student information that is sensitive, protected, or confidential, as provided by state or federal law, is stolen or copied, transmitted, viewed, or used by a person unauthorized to engage in that action.

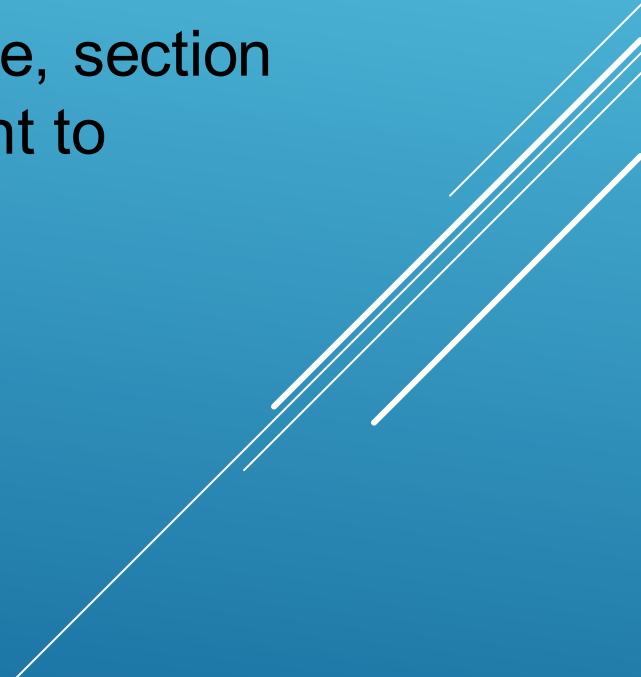
SB 820

(f) The district 's cybersecurity coordinator shall provide notice to a parent of or person standing in parental relation to a student enrolled in the district of an attack or incident for which a report is required under Subsection (e) involving the student 's information.



SB 820 Enforcement

TEA may enforce this provision of the Texas Education Code, section 11.175, through special accreditation investigations pursuant to section 39.057(a)(16).

Decorative white lines consisting of several parallel diagonal strokes in the bottom right corner of the slide.

SB 820

Texas Cybersecurity Framework

Five NIST Functions

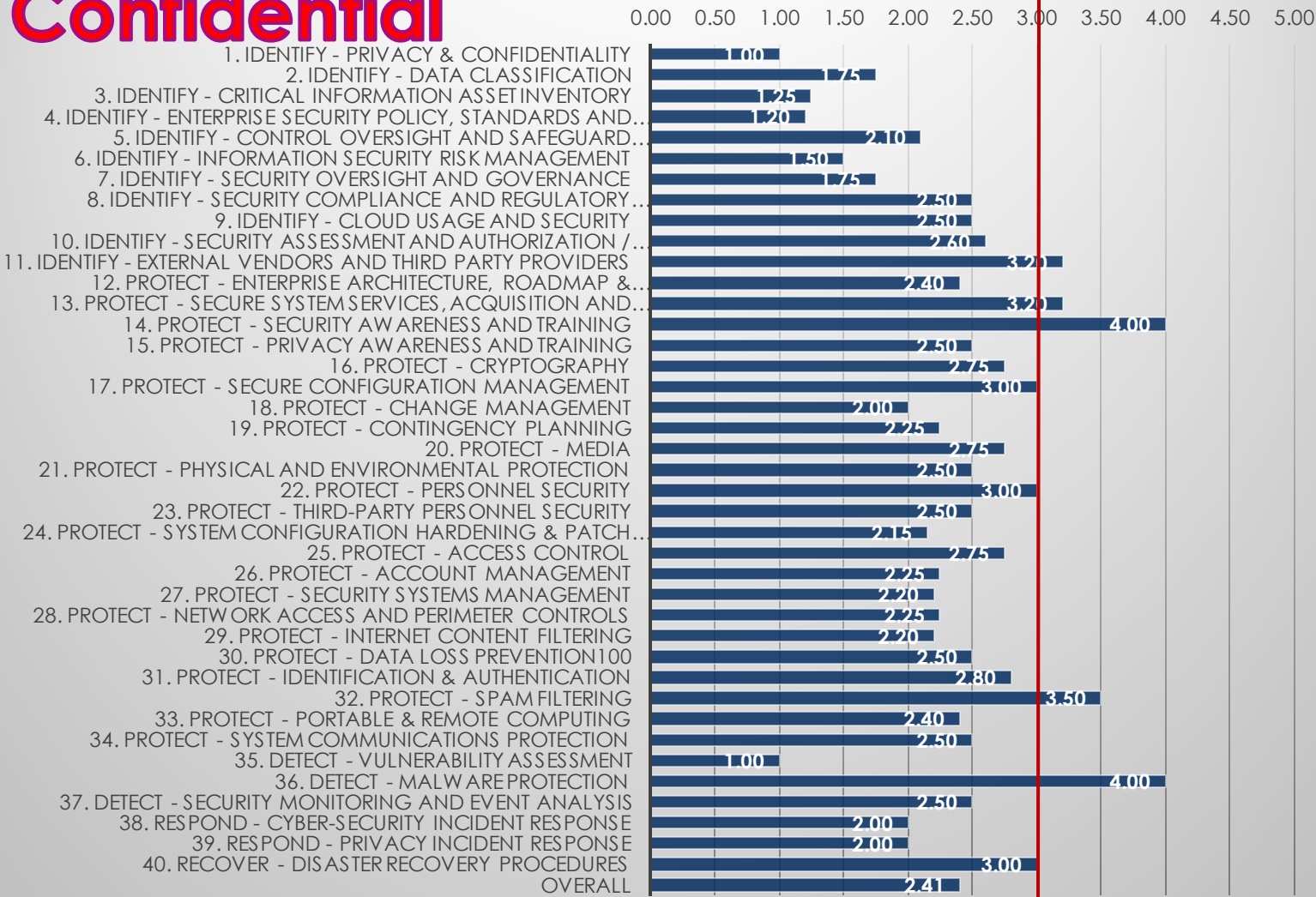
- Identify
 - Protect
 - Detect
 - Respond
 - Recover
- 
- A decorative graphic consisting of several parallel white lines of varying lengths and orientations, located in the bottom right corner of the slide.

SB 820

Texas Cybersecurity Framework Sample 2019

Red Line Indicates Due Diligence 3.25 Monitoring Stage

Confidential



Frameworks which can be considered for SB820

NIST Cybersecurity Framework

<https://www.nist.gov/cybersecurityframework>

CIS RAM (Center for Internet Security® Risk Assessment Method)

<https://learn.cisecurity.org/cis-ram>

CIS CAT Lite (Center for Internet Security® Configuration Assessment Tool)

<https://www.cisecurity.org/blog/introducing-cis-cat-lite/>

Decorative white lines consisting of several parallel diagonal strokes in the bottom right corner of the slide.

Frameworks which can be considered for SB820



EDUCATION (K - 12)

Our commitment to education is unmatched. There is no more virtuous cause than ensuring that our future leaders are able to learn in a secure environment while providing affordable access to leading cybersecurity capabilities.



Small & Medium Business

Understanding the need for Value is at the core of all business, but it is the heart beat of Small and Medium Businesses. We have opened a once inaccessible capability and priced it to win your business.



Enterprise & Higher Education

Ongoing visibility, effectively communicate, reduced risk and developing roadmaps remains elusive and costly for most enterprises. Leveraging technology, and our community of peers, we have unlocked one of cybersecurity's most challenging questions.



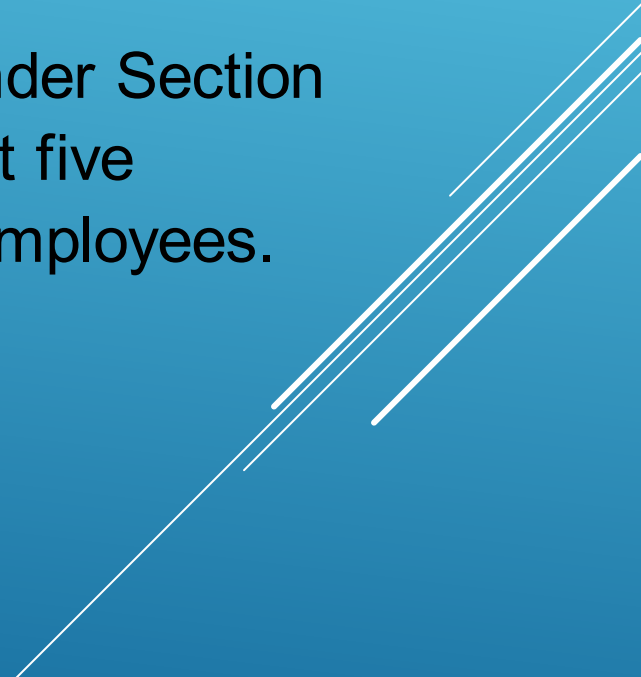
MINERVA

<https://v3cybersecurity.com/>

HB 3834

SECTION 1. The heading to Subchapter N-1, Chapter 2054, Government Code, is amended to read as follows:


Sec. 2054.519. STATE CERTIFIED CYBERSECURITY TRAINING PROGRAMS
DIR, in consultation with the cybersecurity council established under Section 2054.512 and industry stakeholders, shall annually certify at least five cybersecurity training programs for state and local government employees.



HB 3834

Government Code Title 10 Chapter Section 2054.003. DEFINITIONS.

(9) "Local government" means a county, municipality, special district, school district, junior college district, or other political subdivision of the state.



HB 3834

Sec. 2054.5191. CYBERSECURITY TRAINING REQUIRED:

(a-1) At least once each year, a local government shall identify local government employees who have access to a local government computer system or database and require those employees and elected officials of the local government to complete a cybersecurity training program certified under Section 2054.519 or offered under Section 2054.519(f).

HB 3834

(b) The governing body of a local government may select the most appropriate cybersecurity training program certified under Section 2054.519 or offered under **Section 2054.519(f) for employees of the local government to complete.** The governing body shall:

(1) verify and report on the completion of a cybersecurity training program by employees of the local government to the department (DIR); and

(2) require periodic audits to ensure compliance with this section.

- If this Act does not receive the vote necessary for immediate effect, this Act takes effect September 1, 2019.

HB 3834

A list of certified programs is posted DIR's website below:

<https://dir.texas.gov/View-About-DIR/Information-Security/Pages/Content.aspx?id=154>

HB 3834

Statewide Training Requirements

Annual training must be completed by June 14, 2020 by the following employees:

- Local Government (including school districts) Entities: Employees who have access to a local government computer system or database, and elected officials.
- Schools districts should determine definition of employee

HB 3834

How will local governments (including school districts) report training compliance?

- Local government employees will self-report their training compliance using Texas by Texas (TxT). The expected launch date for this application is February 2020.
- In June, DIR will send a detailed report from the TxT application to each local government (including school districts) entity to verify training compliance.
- Although the self-reporting capability will not be available until early February, employees can take their certified cybersecurity training at any time prior to June 14, 2020.

HB 3834

Can a school district file for an exception if we have our own Security Awareness Program?

YES!

A decorative graphic consisting of several parallel white lines of varying lengths, slanted upwards from left to right, located in the bottom right corner of the slide.

HB 3834

Local Government Cybersecurity Training & Awareness Program Exception Form

The cybersecurity officer:

- Has responsibility for information security for their represented organization
- Possesses training and experience required to administer cybersecurity functions
- Has information security duties as their primary duty ("primary" is defined as greater than 50% of the employee's workload).

HB 3834

The training program has been reviewed by the cybersecurity officer and meets the requirements. Refer to the Course Certification Checklist for the detailed list of mandatory course/program topics:

- Requirement 1: Information security habits and procedures that protect information resources
- Requirement 2: Best practices for detecting, assessing, reporting, and addressing information security threats
- Proof of Completion

<https://dir.texas.gov/View-About-DIR/Information-Security/Pages/Content.aspx?id=154>

Questions?

