



Cybersecurity Coordinator Forum (CCF) September 2026

Daniel Ramirez
Chief Information Security Officer
Texas Education Agency
cybersecurity@tea.texas.gov





Before we begin

Three quick notes for a smooth session

WATCH

This webinar is being recorded.

Recording and slides will be posted on the TEA Cybersecurity website a few days after the session.

PARTICIPATE

Chat is off – use Q&A for questions.

We will respond during the webinar if we can or follow up after the webinar by email.

JOIN SECURELY

Use unique login per participant.

Duplicate logins and chatbots are not allowed. AI Notetakers will be removed.

- 1 Team and CCF Introductions
- 2 Legislative Updates
- 3 Cybersecurity Advisories
- 4 Emerging Trends
- 5 K-12 Cybersecurity Initiative Updates
- 6 Other Helpful Information
- 7 Upcoming Events
- 8 Wrap Up



The TEA Team

- Texas Education Agency (TEA) – CISO
 - Daniel Ramirez – Chief Information Security Officer
- TEA K-12 Cybersecurity Initiative Group
 - Julia Schacherl - Executive Director, IT Administration & Compliance
 - Lara Coffey - DCS Contract Manager & K-12 Cybersecurity Project Lead
 - Susan Bain - Sr. Cybersecurity Governance, Risk, & Compliance Analyst
 - Desire Odiwo - Cybersecurity Governance, Risk, & Compliance Analyst
- TEA Security Operations
 - Sam Miller - Cybersecurity Operations Manager
 - Myles Muchineuta - Sr. Cybersecurity Operations Analyst



Daniel Ramirez



Julia Schacherl



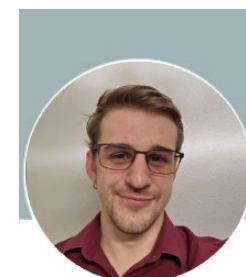
Lara Coffey



Susan Bain



Desire Odiwo



Samuel Miller



Myles Muchineuta

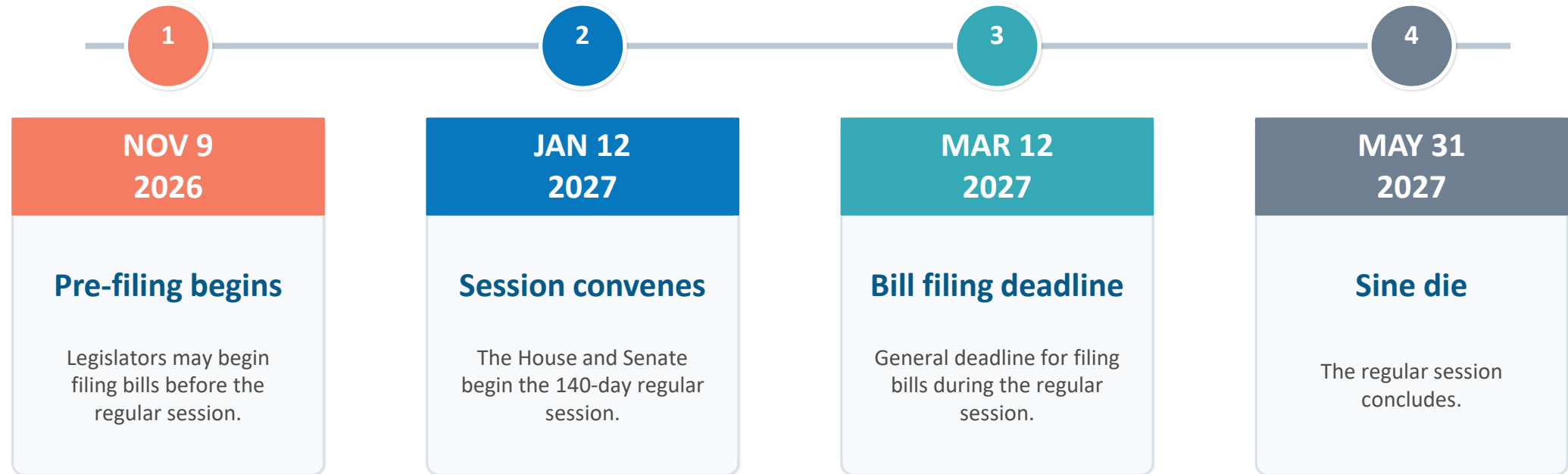
Cybersecurity Coordinator Forum (CCF)

- Monthly TEA forum for K-12 cybersecurity leaders and partners
 - Cybersecurity Coordinators
 - Technology Directors
 - Education Service Centers (ESCs)
 - Regional Security Operations Centers (RSOCs)
- Gain insights from the TEA Information Security Office
- Actionable guidance to strengthen your cybersecurity program
- Stay informed on emerging threats, best practices, and statewide initiatives
- Registration [Link](#) for CCF Forum (use your school email address)
- Mark your calendar for the **fourth Wednesday** of each month at **11am**.

Legislative Updates

90th Legislative Session: What Is Coming Up

Key milestones for Texas school-system cybersecurity leaders



What this means now: Watch for pre-filed bills beginning November 9, track proposals affecting cybersecurity and technology, and plan for rapid review once the session convenes.

90th Legislative Session: Governance Risk and Compliance (GRC) Monitoring Priorities

Legislative updates for K-12 cybersecurity and technology leaders

K-12

K-12-Specific Legislation

What GRC will monitor

- **School-system requirements**
- Bills that may create or change cybersecurity, privacy, reporting, or governance obligations for Texas school systems.
- **AI training**
- Proposals addressing artificial intelligence awareness, responsible use, training, or related compliance expectations.

IT

Technology-Specific Legislation

What GRC will monitor

- **Cybersecurity and data protection**
- Requirements affecting security controls, incident response, data handling, and technology risk management.
- **Technology operations and procurement**
- Proposals that may affect technology acquisition, vendor oversight, digital services, infrastructure, or statewide standards.

CCF takeaway: GRC will track relevant bills, assess potential impacts, and share updates as proposals move through the legislative process.

Cybersecurity Advisories

PivotC2: What School IT Leaders Need to Know

■ Overview

- A report from SOCRadar was recently published about a malicious attack campaign known as "PivotC2" that has so far targeted more than 3,000 IP addresses, resulting in the infection of 178 devices. The majority of the compromises so far are concentrated in the U.S.
- PivotC2 is a custom command-and-control (C2) framework / Remote Access Trojan (RAT) that has been observed being deployed on compromised FortiGate firewalls after exploitation of the Fortinet vulnerability **CVE-2025-25249**. Researchers describe it as a post-exploitation tool designed specifically for organizations that use FortiGate firewalls for perimeter defense and network management.
- CVE-2025-25249 (CVSS* score: 7.3) - Is a heap-based buffer overflow vulnerability in Fortinet FortiOS, FortiSwitch Manager, and FortiSASE that could allow a remote unauthenticated attacker to execute arbitrary code or commands via specifically crafted requests.

*Common Vulnerability Scoring System (CVSS)

PivotC2 Capabilities and Technical Characteristics

- Once installed, PivotC2 can provide attackers with:
 - Interactive remote shell access
 - Command execution
 - File upload and download
 - SOCKS5 and HTTP proxying
 - Port forwarding and network tunneling
 - Internal network scanning
 - Harvesting FortiGate configuration data
 - Collection and decryption of stored credentials and secrets from the firewall
- Researchers report that PivotC2:
 - Is written in Node.js
 - Establishes outbound TLS-encrypted communications to its C2 server
 - Uses multiplexed channels similar to SSH tunneling
 - Supports automated reconnaissance and credential harvesting
 - Appears to contain indicators suggesting AI-assisted development based on code comments and implementation details

PivotC2: Recommended Actions for School Districts

- The primary remediation is to upgrade affected Fortinet software to a fixed version, then investigate for possible compromise because this vulnerability has been actively exploited to deploy PivotC2.

- Determine whether the device was exploited. Because exploitation has been observed in the wild, patching alone may not be sufficient. Investigate for indicators such as:
 - Unexpected outbound TLS connections from the firewall
 - Unrecognized administrative accounts
 - Suspicious scheduled tasks or startup items
 - Evidence of Node.js execution on the appliance
 - Artifacts associated with PivotC2 such as /tmp/.i.js
 - Unexpected configuration exports or credential access activity

PivotC2: Recommended Actions for School Districts

■ Review and Rotate Credentials

Researchers reported that PivotC2 can harvest and decrypt sensitive FortiGate configuration data and stored credentials. If compromise is suspected, rotate:

- Firewall administrator passwords
- SSL-VPN credentials
- LDAP bind accounts
- IPsec VPN pre-shared keys
- Wireless shared secrets
- Service accounts stored on the device

Source: CVE-2025-25249 Exploitation Delivers PivotC2, a FortiGate Post-Exploitation RAT.

Link: [CVE-2025-25249 Exploitation Delivers PivotC2, a FortiGate Post-Exploitation RAT](#)

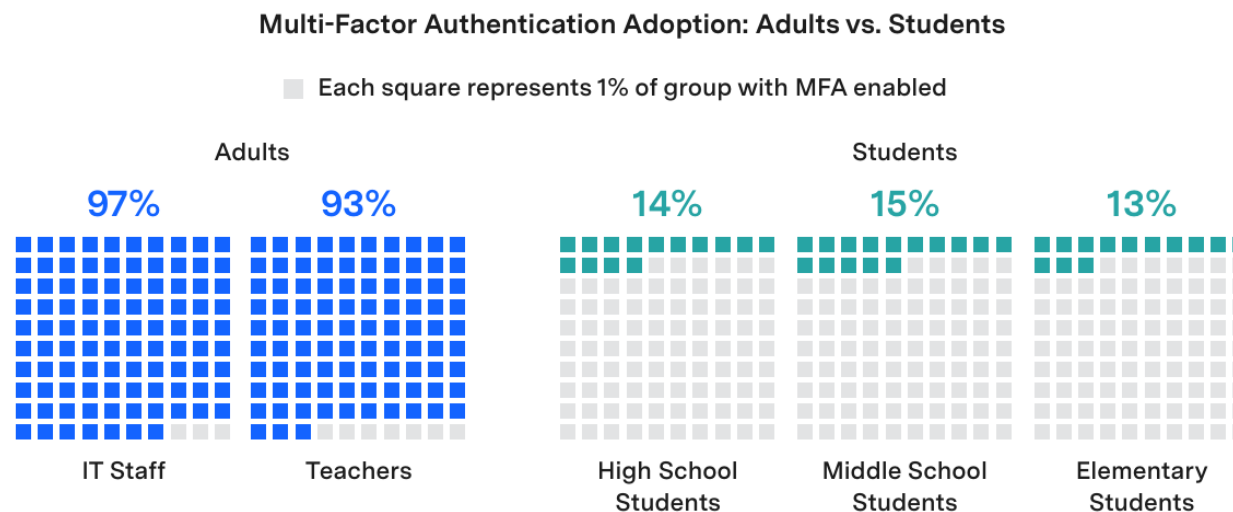
Emerging Threats

K-12 Cyber Incidents

- Cybersecurity incidents up 16% from 2024
 - More than half of school systems in the US (52%) have had an incident in the last year
 - Uptick in Ransomware and Denial of Service (DoS) attacks
 - [K12six.org/map](https://k12six.org/map)
 - Vendor related compromise accounts for large portion of incidents
 - 4% in 2023, now greater than 30% in 2026
 - Lack of funding or support for security tools was listed as a #1 reason for K-12 falling behind in cybersecurity
 - **Take advantage of the K-12 Cybersecurity Initiative**

Source: *Cybersecure 2026 Report by Clever*

- Artificial Intelligence (AI) attacks are extremely prevalent
 - K-12 is a primary target and often labeled as an "Unprepared Sector"
- AI phishing or social engineering attacks have been noted as significantly harder to detect, as well as being more effective



Suspicious Elections Registration

- VoteSafe.org
 - Suspicious election registration website circulating
 - It does not appear to be an official voter registration website.
 - Its appears to harvest user data for political advertising.

VOTE SAFE

We provide you with the information you need to vote with confidence. Sign up for election reminders and get help with voter registration and voting by mail.

 ENTER YOUR ADDRESS



 SELECT YOUR STATE



 REGISTER TO VOTE

Ensure your voice is heard in the next election



 PRE-REGISTER TO VOTE

Under 18? Register as soon as you can!



 CHECK YOUR REGISTRATION

Verify your voter registration status



K-12 Cybersecurity Initiative Updates

K-12 Cybersecurity Initiative (K-12CI)

2023

STATEWIDE LAUNCH

TEA responded as ransomware and cyber threats increasingly targeted Texas schools.

The model pairs sustained public investment with practical, local execution.

BACKED

Funded by the 88th Legislature and continued in the 89th to sustain dedicated cybersecurity resources.

BUILT TO

Provide practical solutions that help schools prevent and respond to major cyber incidents.

FOCUSED

Give priority to high-need school systems.

DELIVERED

Use regional ESC cybersecurity practitioners to help schools implement aligned controls.

K-12CI Current Program Participation

- **School systems that have onboarded with DIR**
 - 566 school systems have signed the DIR interlocal agreement form.
- **Endpoint Detection Response (EDR)**
 - 421 school systems have signed up for EDR, installed on **431,500+** endpoints.
 - **95,000+** attacks blocked. **18,000+** ransomware threats neutralized.
- **Texas Cybersecurity Framework (TCF) Assessments**
 - 77 school systems have signed up; 62 completed.
- **Email Security Service**
 - 263 school systems have signed the ILC with UT-RSOC
 - UT-RSOC has successfully onboarded **232** school systems to the Abnormal AI shared cloud tenant. (TEA = 170, UTRSOC = 62)
- **Security Awareness Training**
 - **437** school systems implemented and active, **171** school systems in onboarding process

For more info on how to sign up, visit [TEA K-12 Cybersecurity](#).

- Realignment Goals:
 - Fully Deploy the EDR Endpoints you need
 - Approved Count will be adjusted down to your deployment level
 - Allow TEA to fully utilize available agents.
 - Only schools deployed at less than 90% will receive report.
- After realignment, you may still request additional endpoints if needed thru the **Add-On** process.
- If you have extenuating circumstances and cannot fully deploy by October 31, notify TEA and your ESC of your delay.

New Initiatives for FY26-FY27

- All school systems are eligible. These services are provided at no-cost to the school system.
- **Implement Email Security Service (Abnormal Security)**
 - Provided in partnership with the University of Texas Regional Security Operations Center (UT-RSOC).
 - Provide 30-day notice to your existing contract holder
 - **Available Now** - [FAQ for Email Security Service](#)
- **DIR Certified Security Awareness Training and Phishing Simulations (InfoSec IQ)**
 - Provided in collaboration with the Technology Alliance for Statewide Initiatives (TASI).
 - **Available Now** - [FAQ for Security Awareness Training](#)
- **Microsoft 365 & Google Workspace Hardening Guides**
 - Developed by TASI to support secure configuration practices.
 - **Available Now** - [Contact your ESC](#) for sign-up and distribution
- **Software Deployment Solution (PDQ Connect Premium)**
 - Provided through TASI to support deployment of EDR agents and other software.
 - **Available October 15, 2026**
- More information about these services can be found on TEA Cybersecurity website.

TASI Updates: K-12 Cybersecurity Initiative Support

- **NEW: Software Deployment and Endpoint Management / Patching Solution**
 - PDQ Connect Premium is available at no cost to your school system
 - PDQ Connect Premium handles software deployment, asset inventory, vulnerability management, patch management, and remote access to assets
 - You can create automations to establish device baselines and document patch / control compliance. Save headaches by deploying pre-built, vetted software packages.
 - **Contact your ESC to sign up. First wave of deployments begins October 15th.**

- **Currently Deploying: Phishing Simulation and Cybersecurity Training**
 - Infosec IQ subscription is available at no cost to your school system
 - Includes current DIR-approved cybersecurity and AI awareness training
 - **Contact your ESC to sign up. Immediately available.**

- **New: Microsoft 365 & Google Workspace Hardening Guides**
 - Developed by TASI to support secure configuration practices.
 - Available Now - [Contact your ESC](#) for sign-up and distribution

- **Continued Services and Support**
 - Assistance with DMARC compliance, MFA, and limited local administrator access.
 - **Contact your ESC for more information**

K-12 Cybersecurity Initiative Regional ESC Contacts

ESC 1 Homar Venecia hvenecia@esc1.net (956) 222-6578	ESC 6 Robert Wyatt rwyatt@esc6.net (936) 435-8276
ESC 2 Marco Mendez marco.mendez@esc2.us (361) 561-8449	ESC 7 Steve Vaughn steve.vaughn@esc7.net (903) 988-6922
ESC 3 Jeff Harris jharris@esc3.net (361) 573-0731 x 1261	ESC 8 Rodney White rwhite@reg8.net (903) 575-2788
ESC 4 Tim Jing tim.jing@esc4.net (713) 744-6847	ESC 9 Michael Chapman Jr. michael.chapmanjr@esc9.net (940) 322-6928
ESC 5 Jerry Wilson jwilson@esc5.net (409) 951-1866	ESC 10 David Mendez david.mendez@region10.org (972) 348-1172

K-12 Cybersecurity Initiative Regional ESC Contacts (cont'd)

ESC 11 Cole Wolsch cwolsch@esc11.net (817) 740-3696	ESC 16 Jandi Tyson jandi.tyson@esc16.net (806) 677-5269
ESC 12 Keith Macik keith.macik@esc12.net (254) 297-1264	ESC 17 Kyle Plumlee kplumlee@esc17.net (806) 281-5851
ESC 13 Rob Jacques rob.jacques@esc13.txed.net (512) 919-5391	ESC 18 Bowen Pugh bowen.pugh@esc18.net (432) 561-4321
ESC 14 Kevin Hill khill@esc14.net (325) 675-8600	ESC 19 Nancy Cruz nchardin@esc19.net (915) 780-5337
ESC 15 Randon Lance randon.lance@esc15.net (325) 481-4081	ESC 20 Dale Harville dale.harville@esc20.net (210) 370-5740

Other Helpful Information

Certified Cybersecurity Training for Texas School Systems

For cybersecurity coordinators, technology leaders, and
school-system administrators



- <https://www.txcc.texas.gov/certified-cybersecurity-training-programs>

Use the current Texas Cyber Command catalog

The certification authority and catalog changed effective September 1, 2026.

FY 2026–2027 certified programs

Texas Cyber Command lists 86 certified programs, including options eligible for K-12 school districts.

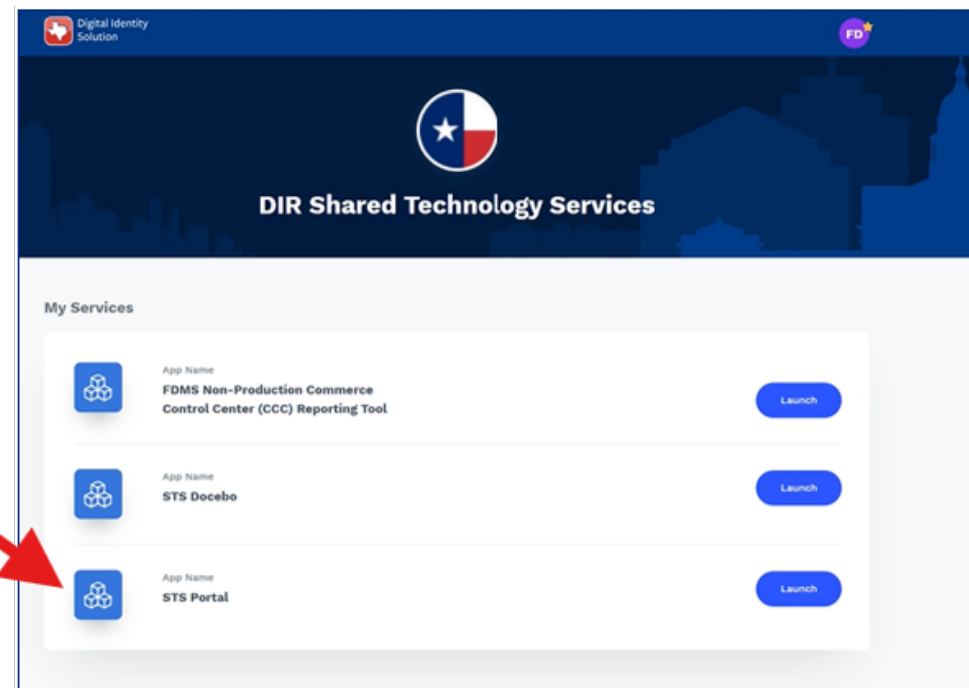
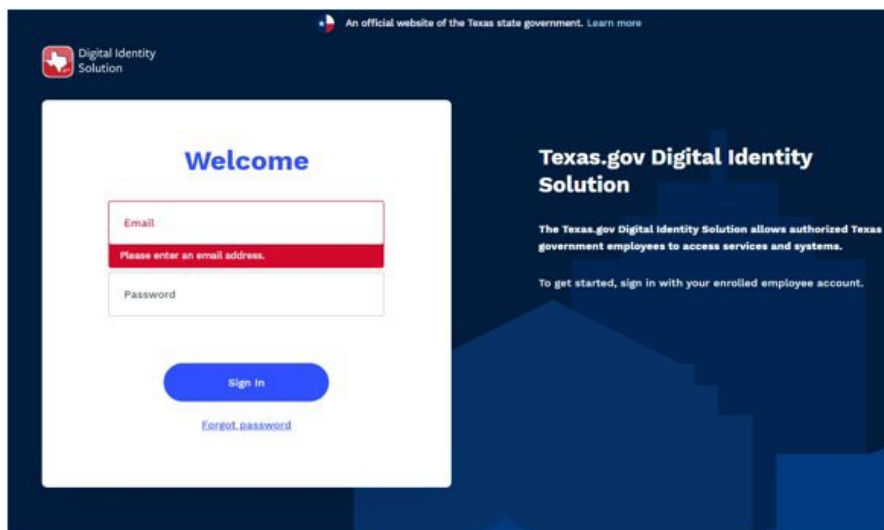
- 1 Filter for your needs**
K-12 eligibility • online/in person • assessment • proof of completion • Spanish • no cost
- 2 Certification scope**
Programs are certified for cybersecurity content. Verify provider details before selection.
- 3 Legacy DIR page**
Useful for prior-year references, but the current catalog is maintained by Texas Cyber Command.



- <https://www.txcc.texas.gov/certified-cybersecurity-training-programs>

Texas Digital Identity Solution - MFA Improvements

- **DIR STS Portal** is now using Texas Digital Identity Solution (TDIS) as the security logon system. This will affect all school systems that currently login to the DIR STS Portal (to request EDR or TCF).
- STS Portal link for TDIS [New portal link for TDIS](#)
- Select the STS Portal tile



TDIS MFA Improvements Project

- Texas Digital Identity Solution (TDIS) is undergoing MFA improvements to modernize and improve the security posture of the platform according to the latest NIST Digital Identity guidelines.

GO-LIVE 12/5/26



Advanced Passkeys and Security Improvements

Passkey MFA is Live in TDIS Portal!

- Passkeys will be supported by the platform as an additional MFA option for a user.
- Registration for these passkeys will be available in the TDIS Portal account settings and during the "New User Enrollment" process.
- Validation using passkeys will also be available in the TDIS Forgot Password workflow.



TDIS Password Policy Changes

- To follow NIST recommendations, TDIS password policies are to allow for all characters and have no complexity or expiration requirements.
- Rules being removed include:
 - At least (1) upper case
 - At least (1) lower case
 - At least (1) number
 - At least (1) special character
 - Password expiration
- Functionality being added includes:
 - ASCII and space characters allowed
 - Word dictionary



Email MFA Removal to Align with NIST Standards

- To align with national standards like NIST, email MFA is to be removed from the platform.
- Email MFA will be removed from all TDIS login flows, including:
 - TDIS Portal
 - Direct Application
- A revamped "New User Enrollment" process will include setting your password and MFA registration.

TDIS Password Policy Changes

Over time, research has shown that while passwords remain common, they are hard for users to choose securely, and **composition rules** (requiring digits/symbols/uppercase) **provide less real-world security benefit** than expected. Longer passwords (such as passphrases) are a reliable way to **improve strength** while deterring account compromise attempts. Passphrases are easier for users to remember compared to short strings with complex rules.

To be compliant with the latest version of NIST 800-63b-4 for passwords, TDIS will be implementing the following changes:

- Accepting of all printing ASCII and space characters
- Removal of password composition rules
- Addition of a “word dictionary” or “password block list” of unacceptable passwords
 - This includes passwords from previous breaches, dictionary words used as passwords, and specific words (e.g., the name of the service itself) that users are likely to choose
- Removal of periodic password changes (password expiration)
 - Users will be required to reset their password if the account is seen to be compromised

TDIS Password Requirements

- ✓ Minimum of 15 characters*
- ✓ Maximum of 64 characters*
- ✗ At least one upper case letter
- ✗ At least one lower case letter
- ✗ At least one number
- ✗ At least one special character (.[@!#\$%^&+=](-_{}))
- ✓ Cannot be in the user's password history (12 most recent)
- ✓ Cannot contain any Personally Identifiable Information
- ✗ Passwords will expire 60 days after the password changed date
- ✓ Passwords cannot be changed within 24 hours of the previous password change

TDIS Improvements – Important Milestones

Phase 1 (Effective August 27th, 2026)

Passkeys added to TDIS platform as an additional MFA option

Phase 2 (Effective Early December, 2026):

Password policies updated to reflect national standards **and**

Email MFA will be removed from the platform

- Users who do not register an additional method prior to the phase 2 go-live will **lose access** to the TDIS Portal and all integrated applications.
- User will need to open a help desk ticket to add an allowable MFA method and restore access after Phase 2 deadline.

AskTED Updates

- Most TEA Cybersecurity emails will be sent to the Cybersecurity Coordinator and/or Technology Coordinator.
- TEA pulls this information from the TEA official contact information portal called AskTED.
- This is located at this link: [AskTED](#). You do not need a logon ID to access this public information.
- Changes to the AskTED portal can only be made by your school's TED Administrator. You can look up your TED Administrator in the AskTED portal.
- Update your AskTED contact information at least once a year and anytime there is a staff change in key positions (Cybersecurity Coordinator or Technology Coordinator).

AskTED - How to Navigate

★ TEXAS EDUCATION AGENCY | TEA Home | TEA District Locator | TEA Index A-Z | TEA Divisions

AskTED

Home | Search by | Quick District Lookup | Reports and Directories | Search RESCs | Administrative Logon | Help

Search by

- School
- District**
- County
- Region
- Texas

Search Criteria: Enter the name of the organization and click **Search**, or click **Pick from List** to select an organization, select desired options, and click **Search**.

District or

or **District Number:**

Organization Status: ☒ Active ☐ Inactive

Information Type: ☐ Organization ☒ Personnel

Include School Principal(s): ☐

Include District Superintendent(s): ☐

Include Other District Roles: ☒ **Select Roles:**

- ATHLETIC DIRECTOR
- BILINGUAL/ESL
- CFO/BUSINESS MANAGER
- CHILD FIND CONTACT
- CURRICULUM
- CYBERSECURITY COORDINATOR**
- DYSLEXIA DESIGNEE
- ESSA/FEDERAL PROGRAMS

Note: To make multiple selections, hold down the **Ctrl** key while clicking on the roles.



AskTED – How to Navigate

TEA Home | TEA District Locator | TEA Index A-Z | TEA Divisions

AskTED

Home

Search by

Quick District Lookup

Reports and Directories

Search RESCs

Administrative Logon

Help

Search by District - Personnel

Search Results for **Conroe ISD**

Revise Search

View Details

Mailing Labels

Email Addresses

3 records found - Select one or more Personnel to Display

Clear Selections

Select All

Clear Sort

Sorted by Ascending Role, Ascending Number

<u>Check to Include</u>	<u>Role▲</u>	<u>Last Name</u>	<u>First Name</u>	<u>Number▲</u>	<u>District Name</u>	<u>County Name</u>	<u>Region</u>	<u>City</u>	<u>Zip</u>
☒	District Person	CYBERSECURITY COORDINATOR	BISBEE	BRIAN	170902	CONROE ISD	MONTGOMERY	06	CONROE 77304
☒	District Person	TECHNOLOGY COORDINATOR	BARTON	ETHAN	170902	CONROE ISD	MONTGOMERY	06	CONROE 77304
☒	District Person	TED ADMINISTRATOR	ANDERSON	GEORGETTE	170902	CONROE ISD	MONTGOMERY	06	CONROE 77304

Revise Search

View Details

Mailing Labels

Email Addresses



AskTED - How to Navigate (cont'd)

 [TEA Home](#) | [TEA District Locator](#) | [TEA Index A-Z](#) | [TEA Divisions](#)

AskTED

[Home](#) | [Search by](#) | [Quick District Lookup](#) | [Reports and Directories](#) | [Search RESCs](#) | [Administrative Logon](#) | [Help](#)

Search by District - Personnel - View Details

[View Detail Results](#)

[Download File](#)[New Search](#)

[View Details](#)[Mailing Labels](#)[Email Addresses](#)

District CONROE ISD (170-902)

[District Type](#)
INDEPENDENT

[CYBERSECURITY COORDINATOR](#)
MR BRIAN BISBEE

[Phone](#)
(936) 709-7656

[Mailing Address](#)
3205 W DAVIS
CONROE, TX 77304

[Fax](#)
(936) 539-1114

[County / Region](#)
MONTGOMERY COUNTY (170) / 06

[Email](#)
bbisbee@conroeisd.net

District CONROE ISD (170-902)

[District Type](#)
INDEPENDENT

[TECHNOLOGY COORDINATOR](#)
MR ETHAN BARTON

[Phone](#)
(936) 709-7627

[Mailing Address](#)
3205 W DAVIS
CONROE, TX 77304

[Fax](#)
(936) 539-1114

[County / Region](#)
MONTGOMERY COUNTY (170) / 06

[Email](#)
ebarton@CONROEISD.NET

District CONROE ISD (170-902)

[District Type](#)
INDEPENDENT

[TED ADMINISTRATOR](#)
GEORGETTE ANDERSON

[Phone](#)
(936) 709-7619

[Mailing Address](#)
3205 W DAVIS
CONROE, TX 77304

[Fax](#)
(936) 709-7612

[County / Region](#)
MONTGOMERY COUNTY (170) / 06

[Email](#)
ganderson@conroeisd.net

Upcoming Events

Upcoming Events

- **October Cybersecurity Coordinator Forum (CCF)**

Oct 28, 2026, 11:00am

Hosted by TEA

Audience: K-12 Cybersecurity Coordinators & Technology Coordinators

Registration: <https://t.ly/Hmimy>

- **ESC 1**

Event: **Cybersecurity Summit 2026**

Date: October 29th

Info: <https://www.esc1.net/cyber-security-summit>

- **ESC 10**

Event: **Cybersecurity Forum**

Date: October 28th

Registration link: [ESC 10 Cybersecurity Forum Registration Link](#)

- **ESC19**

Event: **Sun City Ed Tech Conference**

Date: October 22nd

Info: <https://www.esc19.net/conferences/sun-city-edtech-conference>

- **ESC 20**

Event: **Techtober**

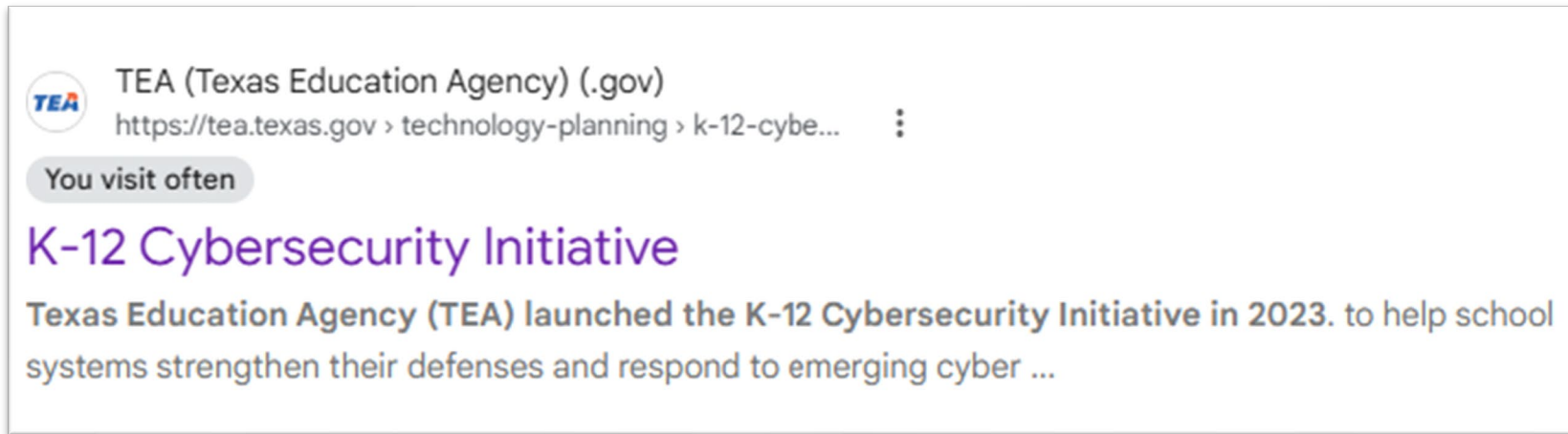
Date: October 22nd – 23rd

Registration Link: [ESC 20 Techtober Registration Link](#)

Wrap Up

K-12 Cybersecurity Initiative Website

- Easy to find → Type **TEA & Cybersecurity** into search engine



- Website: <https://tea.texas.gov/academics/learning-support-and-programs/technology-planning/k-12-cybersecurity-initiative>
 - Steps for onboarding school systems to K-12 Cybersecurity Initiatives
 - New program updates
 - Frequently asked questions
 - Previous K-12 Cybersecurity Initiative Webinars posted on this page
- Program email: k12cyber@tea.texas.gov

Stay Safe & Secure
Thank you!

Questions?

Email:

k12cyber@tea.texas.gov