Cybersecurity Coordinator Forum (CCF)

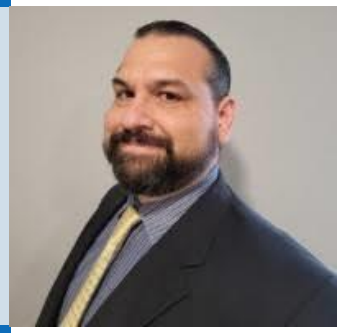
June 2026

Daniel Ramirez

Chief Information Security Officer

Texas Education Agency

cybersecurity@tea.texas.gov



Housekeeping

- Webinar is being recorded.
- Recording and slides will be available a few days after the webinar ends at the TEA Cybersecurity website.
- Chat has been turned off.
- Submit questions in Q&A; we'll address them at the end or follow up by email.
- Duplicate logins are not allowed.
- Chatbots are not allowed; these will be removed if seen.

Agenda

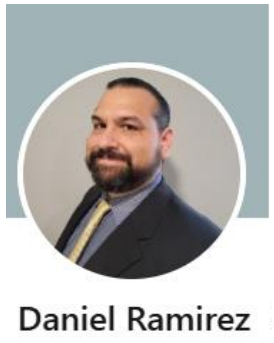
- Team and CCF Introductions – Daniel Ramirez
- Legislative Updates – Daniel Ramirez
- Cybersecurity Advisories – Daniel Ramirez
- Emerging Trends – Sam Miller
- K-12 Cybersecurity Initiative Updates – Daniel Ramirez
- Other Helpful Information – Daniel Ramirez
- Upcoming Events – Daniel Ramirez
- Wrap Up – Daniel Ramirez

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 Coffer - DCS Contract Manager & K-12 Cybersecurity Project Lead
  - Susan Bain - 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 Coffer


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 Chief Information Security Officer
- 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)
- Join the K-12 Cybersecurity Listserv to receive K-12 Cybersecurity Newsletter
- Mark your calendar for the fourth Wednesday of each month at 11am.

Texas Education Agency

Legislative Updates

Important Session Dates and Milestones

- Important dates coming up
  - November 9, 2026 - Pre-filing begins
  - Jan 12, 2027 - House and Senate convene
  - March 12, 2027 - Last day to file bills
  - May 31, 2027 - Sine Die (session is over)

- No new updates

Texas Education Agency

Cybersecurity Advisories

Texas Information Sharing & Analysis Organization (TxISAO)

- In accordance with Texas Government Code Section 2054.0594, DIR created the TxISAO to provide a forum for entities in Texas to share information regarding cybersecurity threats, best practices, and remediation strategies.
- TxISAO is open to all organizations in Texas to include K-12 schools.
- TxISAO participation enables statewide cybersecurity information sharing, improving threat awareness and response coordination across school systems.
- You can sign up for TxISAO at the following link: https://dir.texas.gov/txisao

FortiBleed: What School IT Leaders Need to Know

- Overview
  - A dataset known as "FortiBleed" was reported publicly in June 2026 containing credentials associated with approximately 73,900 FortiGate firewall/Virtual Private Network (VPN) endpoints worldwide.
  - The exposed information reportedly includes firewall management URLs, usernames, and credentials that could be used to target affected organizations.
  - Researchers believe the data may be linked to historical exploitation of previously disclosed Fortinet vulnerabilities and compromised devices that were not remediated.

Even if your district was not directly impacted by the reported credential leak, this event highlights the importance of patching Fortinet devices, restricting management access, and enforcing MFA on administrative accounts.

FortiBleed - Recommended Actions for School Districts

- Verify all FortiGate, FortiProxy, and related Fortinet devices are running supported and fully patched firmware.
- Rotate administrator passwords and VPN credentials, especially if devices were internet-facing or have not been reviewed recently.
- Restrict management interfaces to authorized IP addresses and trusted networks only. Fortinet specifically recommends limiting access to administrative interfaces.
- Implement multi-factor authentication on all external gateways and admin interfaces.
- Review logs for unauthorized administrative activity, unexpected account creation, or configuration changes. Previous Fortinet exploitation activity has included creation of unauthorized administrator accounts.
- Check if your organization is impacted. You can use Hudson Rock's lookup tool: https://www.hudsonrock.com/fortinet

Palo Alto PAN-OS GlobalProtect Authentication Bypass

- Palo Alto Networks disclosed CVE-2026-0257, an authentication bypass vulnerability affecting GlobalProtect VPN portals and gateways in PAN-OS. An attacker can bypass normal authentication controls and establish an unauthorized VPN connection into a network.
- The vulnerability has been actively exploited in the wild and was added to CISA's Known Exploited Vulnerabilities (KEV) catalog.
- Impacted organizations are those using Palo Alto GlobalProtect VPN on affected PAN-OS versions.
- Successful exploitation allows an unauthenticated attacker to gain VPN access and potentially reach internal resources without valid credentials.
- Because GlobalProtect is typically internet-facing, affected systems are attractive targets for attackers.

What Should School Systems Do?

- Immediately verify PAN-OS and GlobalProtect versions.
- Apply Palo Alto's security updates for affected systems.
- If patching cannot occur immediately:
  - Disable Authentication Override, or
  - Configure a dedicated certificate exclusively for Authentication Override
- Review GlobalProtect logs for indicators of unauthorized VPN activity.

This is an actively exploited VPN authentication bypass vulnerability. School districts using Palo Alto GlobalProtect should prioritize patching and review whether Authentication Override is enabled.

Source: Palo Alto Networks Security Advisory CVE-2026-0257 and Unit 42 Threat Brief.

Link: https://security.paloaltonetworks.com/CVE-2026-0257

Texas Education Agency

Emerging Threats

Threat Nomenclature

- Nation-state threat actor groups are given names based on their region.
- Fancy Bear is a threat group based out of Russia, indicated by the animal bear (CrowdStrike).
- Midnight Blizzard is a threat group also based out of Russia, but is instead indicated by the weather type (Microsoft).
- Look up these threat actor groups and understand which world regions are active.

LLM and AI Based Attacks – Prompt Injection

- Emerging attack vector used to trick LLMs into generating feedback that may expose unintended information, break out of security boundaries, or return malicious results.
- Commonly used when users can submit outside information to a potentially automated process
- Prevented by limiting use of automated AI prompting, AI regulation security software, and AI data access controls
- Example: **CVE-2025-32711**

*Large Language Models (LLM) – Artificial Intelligence (AI)

LLM and AI Based Attacks – Token Smuggling

- Similar to prompt injection, can be used in conjunction
- Using encoded prompts to bypass safety features limited to human language
- Usually requires (but not always) direct access to an LLM with internal information access

Mythos Updates

- Federal directive to Anthropic to disable Fable 5 and Mythos 5 submitted on June 12th
- Fable 5, before being disabled, was a publicly available, and promotionally free, version of Mythos.
- Relatively low safeguards which lead to the Federal directive
- Vulnerability exploitation will speed up exponentially as these models are released.

Texas Education Agency

K-12 Cybersecurity Initiative Updates

TEA K-12 Cybersecurity Initiative

- TEA launched the K-12 Cybersecurity Initiative in 2023 to address rising ransomware and cyber threats targeting Texas schools.
- The initiative is funded by the 88th Legislature and continued in the 89th to support dedicated cybersecurity resources.
- It provides practical solutions to help schools prevent and respond to major cyber incidents.
- Priority is given to high-need school systems.
- Regional ESC cybersecurity practitioners are available to assist schools with implementing controls aligned to the initiative.

Current Program Participation

- **School systems that have onboarded with DIR**
  - **548** school systems have signed the DIR interlocal agreement form.

- **EndPoint Detection Response (EDR)**
  - **412** school systems have signed up for EDR, installed on **372,500** endpoints.
  - **54,000+** attacks blocked. **17,000+** ransomware threats neutralized.

- **Texas Cybersecurity Framework (TCF) Assessments**
  - **72** school systems have signed up; **52** completed.

- **Email Security Service**
  - **119** school systems have signed the ILC with UT-RSOC
  - UT-RSOC has successfully onboarded **88** school systems to the Abnormal AI shared cloud tenant. (TEA = 60, UTRSOC = 28)

- **Security Awareness Training**
  - **298** school systems implemented and active, **263** school systems in onboarding process

For more info on how to sign up for EDR & TCF, visit TEA K-12 Cybersecurity.

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).
  - **Available Now - FAQ**
- **DIR Certified Security Awareness Training and Phishing Simulations (InfoSec IQ)**
  - Provided in collaboration with the Technology Alliance for Statewide Initiatives (TASI).
  - **Available Now - FAQ**
- **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** for EDR and Other Applications (TBD)
  - Provided through TASI to support deployment of EDR agents and other software.
  - **Available September 1, 2026**

- More information about these services can be found on TEA Cybersecurity website.

Email Security Service - Benefits

- AI-driven email protection that protects organizations from phishing, business email compromise, and account takeover attacks by analyzing behavioral anomalies rather than relying on traditional email filtering rules
- Integrates directly with Microsoft 365 or Google Workspace via application program interface (API); does not require changes to mail exchange records
- Easy implementation—minimal work effort for schools
- New FAQ has been published on TEA Cybersecurity website
- If you are already receiving RSOC services from UT-Rio Grande Valley (RGV) or Angelo State, please let UT-RSOC know, and they will coordinate this service with your existing RSOC

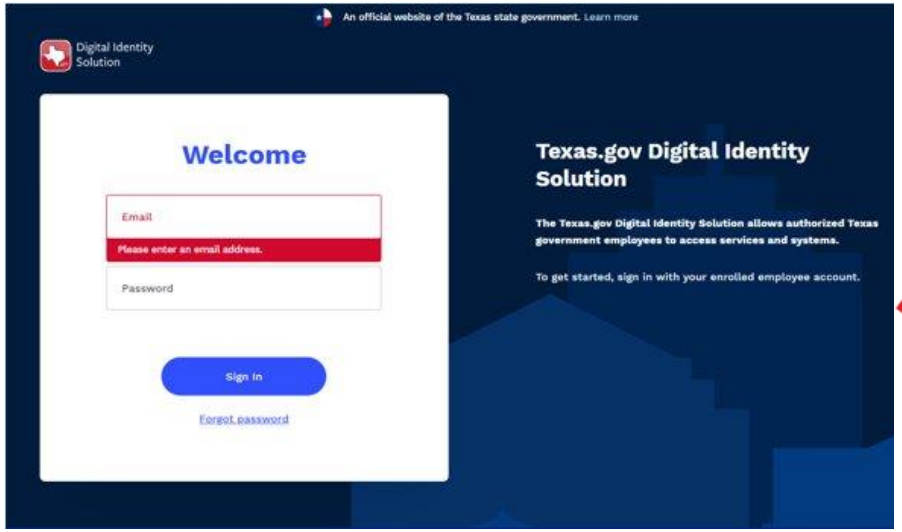
Texas Education Agency

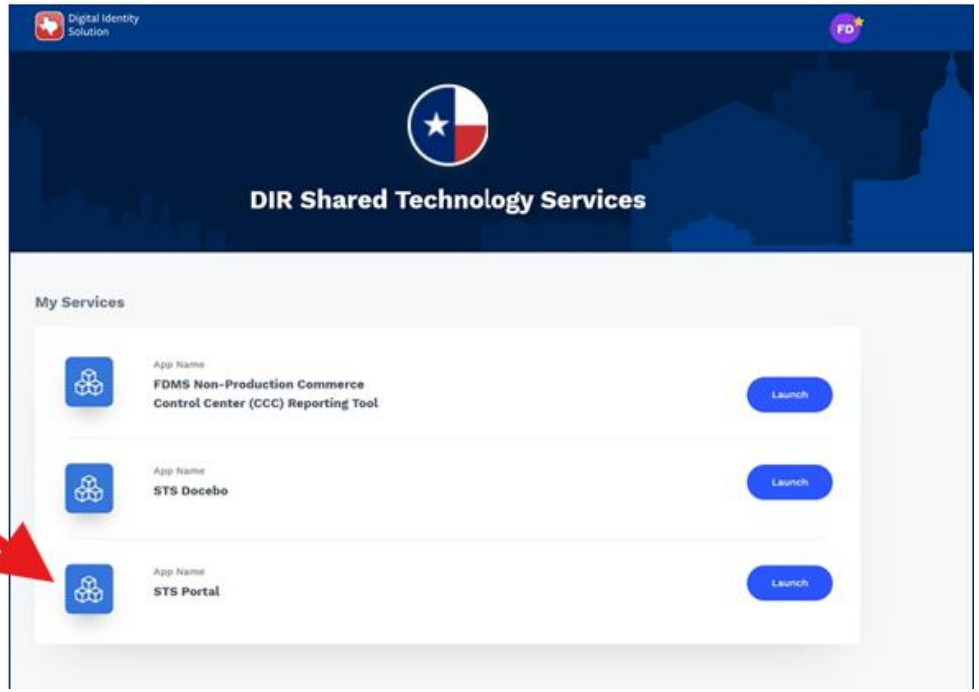
Other Helpful Information

DIR STS Portal transition to Texas Digital Identity (TDIS)

- **DIR STS Portal** is transitioning to Texas Digital Identity Solution (TDIS) on **June 28**. This will affect all school districts that currently login to the STS Portal as credentials will change.

- New portal link for TDIS New portal link for TDIS
- Select the STS Portal tile





TDIS Transition – Users who need TDIS credentials

Path #1 – STS portal user who doesn't have a TDIS credential:

- **Action needed by You for TDIS Enrollment in Production environment**
- The **enrollment e-mails** will go out during the Production environment migration on **Sunday, June 28, 2026** to active STS Portal users.
- The enrollment email will be sent from: **no-reply@myaccess.dir.texas.gov** with the subject **Texas Digital Identity Solution | Enroll your Account**, including your TDIS User ID and instructions to enroll to the Production environment.
- Please add this email address to your safe list or check your Junk Email folder in Outlook, if it does not appear in your Inbox.
- The initial enrollment window is only **open for 72 hours**.
- Please contact STS Service Desk at stshelp@sharedtechnologyservices.texas.gov or 1-877-767-0656 if the enrollment email needs to be resent.

TDIS Transition - Users who already have TDIS credentials

Path #2 – STS Portal user who does have a TDIS credential:

- After June 28, when you click on the STS Portal link, you will be forwarded to TDIS Login screen.
- Use your existing TDIS credentials (same ones you use for logging into SPECTRIM)
- If user is already currently enrolled in TDIS (for accessing Enterprise applications like CAPPS, SPECTRIM), they will NOT receive an enrollment e-mail. They will continue to use their existing TDIS credentials to access STS portal.
- Update your bookmarks. TDIS Login
- Please contact STS Service Desk at stshelp@sharedtechnologyservices.texas.gov or 1-877-767-0656 if you experience any trouble logging in.

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 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 AskTED 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).

Texas Education Agency

Upcoming Events

Upcoming Events

- No CCF Meetings in July & August, will resume in September

- **September Cybersecurity Coordinator Forum (CCF)**
  - Sept 23, 2026, 11:00am
  - Hosted by TEA
  - Audience: K-12 Cybersecurity Coordinators & Technology Coordinators
  - Registration: https://t.ly/Hmimy

Texas Education Agency

Wrap Up

K-12 Cybersecurity Initiative Website

- Easy to find → Type **TEA** & **Cybersecurity** into search engine—it's the first link
- https://tea.texas.gov/academics/learning-support-and-programs/technology-planning/k-12-cybersecurity-initiative
  - Steps for onboarding school systems to DIR Shared Technology Services (STS) portal
  - Updates about the program
  - Frequently asked questions about the program
  - 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