Cybersecurity Coordinator Forum

April 2026

Daniel Ramirez

Chief Information Security Officer

Texas Education Agency

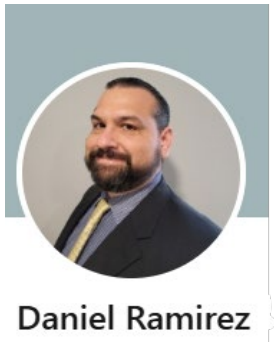
cybersecurity@tea.texas.gov

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.

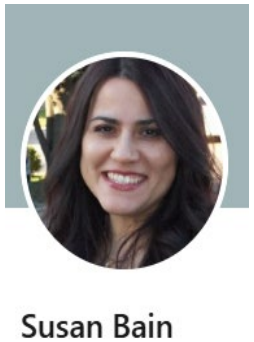
The TEA Team

- 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 - Cybersecurity Operations Associate

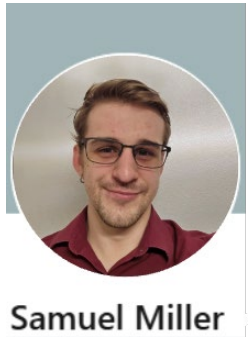

Daniel Ramirez


Julia Schacherl


Lara Coffer


Susan Bain


Desire Odiwo


Samuel Miller


Myles Muchineuta

Cybersecurity Coordinator Forum (CCF)

The **TEA Cybersecurity** team hosts a **monthly** meeting for Texas school system **Cybersecurity Coordinators, Technology Coordinators**, Education Service Center (ESC) **Cybersecurity personnel**, and other members of the community that support K-12 Cybersecurity efforts. It provides content designed to assist school systems and ESCs towards maturity in an information security program.

Agenda

- Introductions & Housekeeping – Daniel Ramirez
- Legislative Updates – Susan Bain
- Cybersecurity Advisories – Myles Muchineuta & Sam Miller
- K-12 Cybersecurity Initiative Updates – Daniel Ramirez
- Upcoming Events – Daniel Ramirez
- Wrap Up – Daniel Ramirez

Texas Education Agency

Legislative Updates

Important Session Dates and Milestones

- 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)

Artificial Intelligence (AI) Focus During Session

- AI & Data Privacy are confirmed priorities for the 90th Texas Legislative Session
- The Texas House Interim Committee Charges released in March 2026 explicitly instructs committees to study:
  - Artificial intelligence–related technologies
  - Data centers and advanced computing infrastructure
- This signals likely new legislation and amendments to:
  - Texas Responsible Artificial Intelligence Governance Act (TRAIGA)
  - Texas Data Privacy and Security Act (TDPSA)
- Focus on governance, deployment limits, and oversight of emerging technologies

Note: TEA will be monitoring guidance that may emerge from the 90th Legislative Session and will not issue guidance in advance of the session.

Current Cybersecurity Awareness Training Requirements

- Texas Government Code § 2054.5191
  - Annual cybersecurity awareness training
  - Training must be certified by Texas DIR
  - Annually certify compliance by August 31
  - K-12: Cybersecurity Coordinator, and Elected Officials

- HB 3512 (89R) added an annual AI awareness training requirement

AI Training Program Certification

- Government Code Section 2054.5193(b) states that an artificial intelligence training program must:
  - focus on forming an understanding of how artificial intelligence technology may be used in relation to a state employee's responsibilities and duties; and
  - teach best practices on literacy in deploying and operating the artificial intelligence technologies.

AI Awareness Training Requirements

- School Systems
  - Only cybersecurity coordinator required to complete annual AI training
  - Elected officials are subject to local government training requirements.
  - Any other school system employee as determined by school system and cybersecurity coordinator

- State Agencies/Local Governments
  - Employees who use a computer at least 25% of employee's required duties
  - Elected or appointed officers/officials
  - State agency contractors will NOT be required to complete AI training

DIR Certified AI Training Programs

- DIR has certified several AI training programs. https://dir.texas.gov/statewide-artificial-intelligence-ai-awareness-training
  - Vendor-Provided Training – 16 certified
    - 14 which require a registration fee
    - 2 which are no cost
  - Public Sector-Provided Training – 10 certified
    - 2 which require a registration fee
    - 8 which are no cost

- Due August 31, 2026
- Keep a record of completion for auditing purposes

Texas Education Agency

Cybersecurity Advisories

Trends: Threat Landscape

- 89% Increase in AI-enabled attacks
- This has caused a drastic decrease in breakout time, just 29 minutes! (Down 65% from 2024)
- Malware is seen less, only 18% of attacks were malware related in 2025
- 24 new threat adversaries were seen and acknowledged by major Cybersecurity firms
- A 42% increase in Zero Day attacks being exploited before public disclosure has been observed since 2025
- Account compromise is on the rise and has seen a 36% increase

Source: CrowdStrike's 2026 Global Threat Report

Advisory: Iran Conflict

- Iranian based advanced persistent threats (APTs) increasingly active.
- Due to the current Iranian conflict, there has been an uptick in malicious Iranian cyberattacks.
- These attacks are mainly targeted at critical infrastructure and government agencies, but caution is advised for all US cybersecurity programs.
- Creating advanced detection or block rules for Iranian based traffic is advised while the conflict persists.

Source: https://www.cisa.gov/news-events/cybersecurity-advisories/aa26-097a

Advisory: Adobe Product Vulnerability

- Multiple Vulnerabilities have been discovered in Adobe Products
- The most severe of these is a remote code execution
- It is recommended to update all Adobe products to the most recent stable patch
- This affects the following Products:
  - Adobe Bridge
  - Adobe Dreamweaver
  - Adobe InDesign
  - Adobe InCopy
  - Adobe Photoshop
  - Adobe Illustrator
  - Adobe Substance 3D
  - Adobe Cold Fusion

Source: https://www.cisecurity.org/advisory/multiple-vulnerabilities-in-adobe-products-could-allow-for-arbitrary-code-execution_2026-005

Advisory: AI-Enabled Threats

- Social Engineering
  - AI has given threat actors the ability to create increasingly complex social engineering attacks as well as stand up full web infrastructure to phish users in minutes
  - It is necessary more than ever to monitor for phishing and train users to be phishing resistant
- Information Operations
  - As AI capabilities evolve, legitimate information is harder to verify. AI is being used to spread disinformation with false images and videos
  - Ensuring information is accurate and verified before sharing is now more difficult and more critical
- Technical Operations
  - Threat actors have begun using AI to write malicious code and exploits
  - Stay on top of vulnerability management and patch management

Source: CrowdStrike's 2026 Global Threat Report

Texas Education Agency

Emerging Threats

Widespread MacSync Stealer Campaign Impacting SLTT macOS Users

- The Center for Internet Security (CIS) has identified an active and evolving macOS infostealer campaign, MacSync Stealer, that is specifically impacting State, Local, Tribal, and Territorial (SLTT) environments.
  - The campaign relies on ClickFix social engineering, search engine optimization (SEO) poisoning, and in-memory malware execution to bypass traditional macOS security controls and steal sensitive data at scale.
  - MacSync Stealer is a macOS infostealer offered as Malware-as-a-Service (MaaS).
  - Threat actors target users via fake CAPTCHA pages and search engine results, tricking victims into copy-pasting malicious commands into the Terminal (ClickFix technique).
- The campaign has evolved significantly in 2026, shifting from detectable binaries to:
  - Shell-based loaders
  - AppleScript execution via trusted macOS components
  - Entirely in-memory execution

Source: MS-ISAC / Center for Internet Security (CIS).

Date: April 2026 | Traffic Light Protocol (TLP): GREEN

Widespread MacSync Stealer Campaign Impacting SLTT macOS Users

- Critical Threat:
  - High Business Impact: Stolen credentials and session tokens can enable follow-on compromise of email, virtual private network (VPN), cloud services, and internal systems.
  - Mac-Focused Threat: This campaign specifically targets macOS users, a platform often perceived as lower risk and therefore less monitored.
  - Human-Enabled Entry Point: The attack abuses normal user behavior, reducing the effectiveness of technical controls alone.
- The malware steals:
  - Browser credentials and session data
  - macOS Keychain contents
  - Cloud credentials (AWS, Kubernetes, secure shell (SSH))
  - Sensitive files (PDFs, keys, VPN configs, etc.)
  - Cryptocurrency wallets (including persistent ledger hardware wallet backdooring)

Widespread MacSync Stealer Campaign Impacting SLTT macOS Users

How the Attack Works (At a High Level)

1. Malicious Search Results
   - Attackers manipulate search engine results to promote fake but legitimate-looking websites.
   - Users searching for common content (ebooks, tools, technical guidance) are redirected to attacker-controlled pages.
2. Fake CAPTCHA & “ClickFix” Technique
   - Victims encounter a fake CAPTCHA page instructing them to copy/paste command into the macOS Terminal.
   - This approach bypasses typical malware download warnings because the user executes the command.
3. Silent Data Theft
   - Once executed, the malware runs invisibly and steals:
     - Browser cookies and saved passwords
     - macOS Keychain credentials
     - Cloud and developer credentials (AWS, SSH, Kubernetes)
     - Sensitive documents and local files
   - Stolen data is exfiltrated and local traces are removed.
4. Advanced Persistence Risk
   - In some cases, the malware modifies installed cryptocurrency wallet applications, allowing long-term credential theft even after the main malware is removed.

Widespread MacSync Stealer Campaign Impacting SLTT macOS Users

- Mitigation Strategy - The Center for Internet Security (CIS) strongly recommends:
  - User awareness training focused specifically on ClickFix / fake CAPTCHA attacks
  - DNS-level blocking of known malicious domains (MDBR - Malicious Domain Blocking and Reporting)
  - Endpoint detection & response (EDR) & managed detection & response (MDR) with script execution controls
  - Strict application allowlisting
  - Limiting Full Disk Access on macOS
  - Keeping macOS fully up-to-date (newer versions include Terminal paste warnings)
  - Subscribing to MS-ISAC Indicator Sharing

- CIS assesses it is highly likely this technique will continue throughout 2026 due to its speed, scalability, and low cost.

More information can be found below: RSA Archer GRC Platform

Re-emerging Microsoft Exchange Vulnerability

- A critical vulnerability in Microsoft Exchange Server (2013, 2016, 2019), CVE-2023-21529, initially discovered in 2023, has recently re-emerged as a significant threat.
- This flaw enables Remote Code Execution (RCE) and has been highlighted in ongoing analyses of Exchange exploitation techniques, including those associated with ProxyNotShell-style attack chains.
- Impacted Versions:
  - Microsoft Exchange Server 2013 Cumulative Update 23
  - Microsoft Exchange Server 2016 Cumulative Update 23
  - Microsoft Exchange Server 2019 Cumulative Update 11
  - Microsoft Exchange Server 2019 Cumulative Update 12

Source: Texas Department of Information Resources (DIR)

Date: April 2026 | PUB0006848

Re-emerging Microsoft Exchange Vulnerability

- **Impact:** The vulnerability allows an authenticated attacker to execute arbitrary code on the target server through specially crafted requests that exploit insecure deserialization mechanisms within the Exchange Server application.

- **Mitigation:** Microsoft has released security updates to address CVE-2023-21529. Organizations should consult the Microsoft CVE-2023-21529 Advisory for specific patch details and apply the appropriate updates for the Exchange Server version. The security updates address the deserialization vulnerability by implementing proper input validation and sanitization of serialized data.

- Evaluate your environment for any affected Exchange Servers and take immediate actions to remediate.

DIR Reported K-12 Incident Trends, Jan-Apr 2026

Email & Phishing threats account for a majority of recent K-12 security incidents, reflecting a continued rise in phishing and malicious email activity.

Incident ID	Discovery Date	Issue
INC-11672	4/9/2026	email inadvertently sent by teacher
INC-11670	4/8/2026	Phishing link
INC-11669	4/1/2026	Phishing link
INC-11668	4/6/2026	Attacker gained access to user acct. Acct used to send phishing links.
INC-11667	4/3/2026	Phishing link
INC-11665	4/1/2026	Phishing link
INC-11663	4/1/2026	DDoS
INC-11660	3/30/2026	Phishing link from a known person who's account had been Phished
INC-11657	3/31/2026	Look alike domain created
INC-11654	3/26/2026	Phishing link
INC-11652	3/23/2026	Phishing link
INC-11650	3/24/2026	Ransomware
INC-11642	3/7/2026	Phishing link
INC-11638	3/3/2026	Acct compromise. Unknown origin.
INC-11636	3/2/2026	Phishing link
INC-11634	3/2/2026	Phishing link
INC-11633	2/17/2026	Phishing email sent from teacher account to students
INC-11628	2/23/2026	Phishing link
INC-11626	2/19/2026	Phishing link
INC-11614	1/29/2026	Phishing link
INC-11611	1/28/2026	account compromise

Texas Education Agency

K-12 Cybersecurity Initiative Updates

TEA K-12 Cybersecurity Initiative

- In 2023, Texas Education Agency (TEA) launched the **K-12 Cybersecurity Initiative** in response to the increasing threat of ransomware and other malicious cyber activity targeting school systems across Texas.
- The initiative was made possible through funding approved by the 88th Texas Legislature and continued in the 89th session which continued TEA's request for **dedicated cybersecurity resources** to help school systems strengthen their defenses and respond to emerging cyber risks.
- The goal of the initiative is to deliver immediate, practical solutions to help school systems defend against major cyber incidents, such as ransomware attacks.
- Priority is given to high-need school systems.
- Cybersecurity practitioners are available through regional education service centers (ESCs)to support the implementation of cybersecurity controls aligned with the scope of this initiative.

Current Program Participation

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

- **End Point Detection Response (EDR)**
  - 391 school systems have signed up for EDR.
  - Installed on 316,500 endpoints.
  - **51,000+** attacks blocked.
  - **17,000+** ransomware threats neutralized.

- **Texas Cybersecurity Framework (TCF) Assessments**
  - 71 LEAs have signed up; 52 completed.
  - Individual results from the assessments are kept confidential.

- **Network Detection Response (NDR) pilot**
  - Nine LEAs have implemented NDR pilot.
  - Pilot is closed to new customers while pilot benefits & costs are evaluated.

Current Program Participation

- **Multi-Factor Authentication (MFA)**
  - 702 school systems indicated interest in implementation assistance in 2024
  - 319 (45%) of those school systems have since implemented MFA

- **Email Security Protocol (ESP/DMARC*)**
  - 784 school systems indicated interest in implementation assistance in 2024
  - 167 (21%) of those school systems have since implemented ESP

- **Limited Local Administrator Access (LLA)**
  - 684 school systems indicated interest in implementation assistance in 2024
  - 202 (29%) of those school systems have since implemented LLA

* DMARC (Domain-based Message Authentication, Reporting, and Conformance)

New Services Being Added – at no cost to schools

- **Cloud Email Security** – Provided in collaboration with the University of Texas (UT) Regional Security Operations Center (RSOC). **Available May 1.**
- **Security Awareness Training** and **Phishing Simulations** – Provided in collaboration with the Technology Alliance for Statewide Initiatives (TASI). ESCs will send signup info to schools **May 13.**
- **Microsoft365 & Google Workspace Hardening Guides** – Under development by TASI. ESCs will send program information/signup information to schools **June 1.**
- **Software Deployment Solution** for rollout of EDR agents and other software – provided in collaboration with TASI. **Available Sept 1.**

Email Security Service - New Service Available

- Email Security Service available **May 1**.
- Partnership with UT-RSOC using their existing email security service Abnormal AI (previously called Abnormal Security).
- No cost to schools. All schools are eligible.
- Must complete an **Interest & Pre-registration Survey** (sent 4/21 at 1pm to Superintendent, Tech & Cybersecurity Coordinators)
- Purpose of Interest & Pre-registration Survey.
  - If your school is interested, we want to know your # of licenses needed and your target implementation timeframe.
  - If your school is not interested, we want to know that too. This is our way of verifying that your school is aware of the program.

Email Security Service - Benefits

- AI-driven email protection that detects threats that traditional tools often miss, such as executive impersonation, vendor invoice scams, and phishing attempts with no links or attachments.
- It 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.
- Interlocal Contract (ILC) with UT-RSOC required.
- Pre-registration required.
- 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.

Email Security Service - Implementation Timeline

Phase 1: Administrative Setup & Intake (Typically ~5 business days + ~10 minutes effort)

- ILC reviewed, signed, and returned to UT *(timeline varies by school system, but typically ~5 business days)*
- Onboarding form completed (captures user count, email platform, and key details) *(~10 minutes)*

Phase 2: Integration & Initial Data Ingestion (~2–24 hours total + ~5–10 minutes per integration)

- Integration link sent to designated point of contact and completed *(~5–10 minutes per email platform; separate links required for O365 and Google if both are used)*
- Initial data ingestion and dashboard availability *(~2–24 hours after integration)*
- User account creation and welcome communication

Phase 3: Passive (Alert-Only) Mode (Minimum ~10 days)

- System operates in alert-only mode to baseline environment and allow optional dashboard familiarization
- Abnormal builds behavioral understanding of users and email patterns

Phase 4: Transition to Active Protection (~24 hours after activation + ~5–10 minutes setup)

- Activation link deployed to enable full protection *(~5–10 minutes)*
- Full enforcement and protection enabled *(~24 hours after activation)*

Phase 5: Ongoing Monitoring & Tuning (Ongoing; initial tuning within first few days)

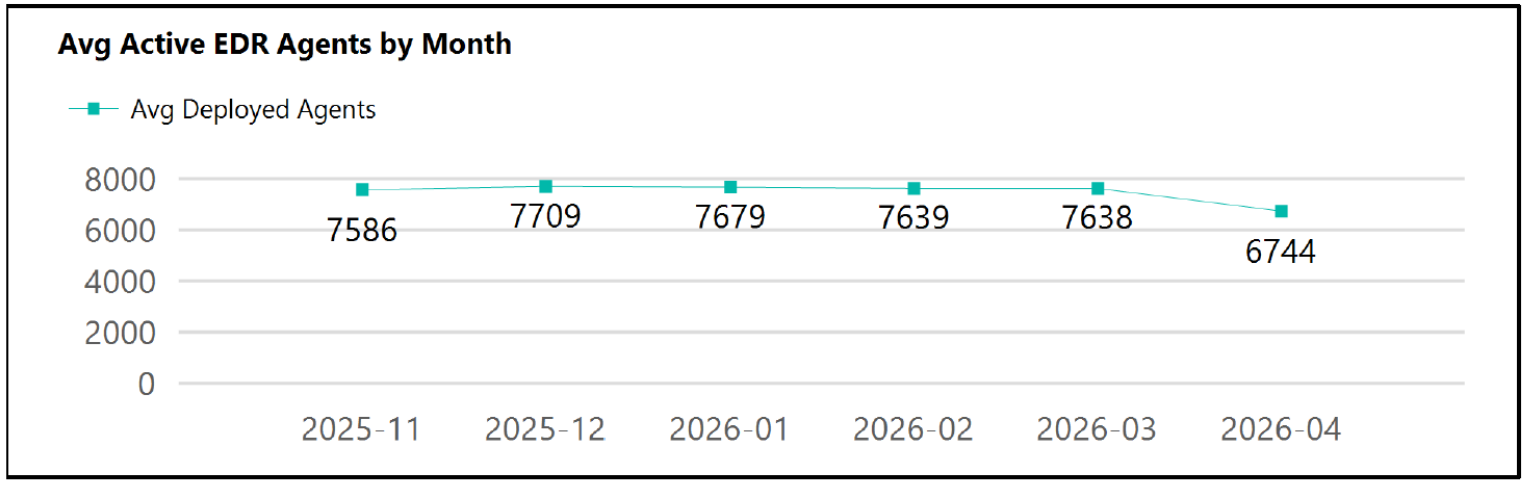
- Continuous monitoring, tuning, and optimization based on findings and organizational needs

EDR Realignment

- Target Date: May 1, 2026
- Adjusting the approved count
- Email from doNotReply@tea.texas.gov
- Emails sent to Superintendent & Technology Coordinator
  - Report will show current approved count & deployment

As part of the K-12 Cybersecurity Initiative, our records show that your school system is currently below 90% deployment of your approved EDR agent allocation.

Approved Agents = 10000, Currently Deployed Agents = 6930 [69.30%]

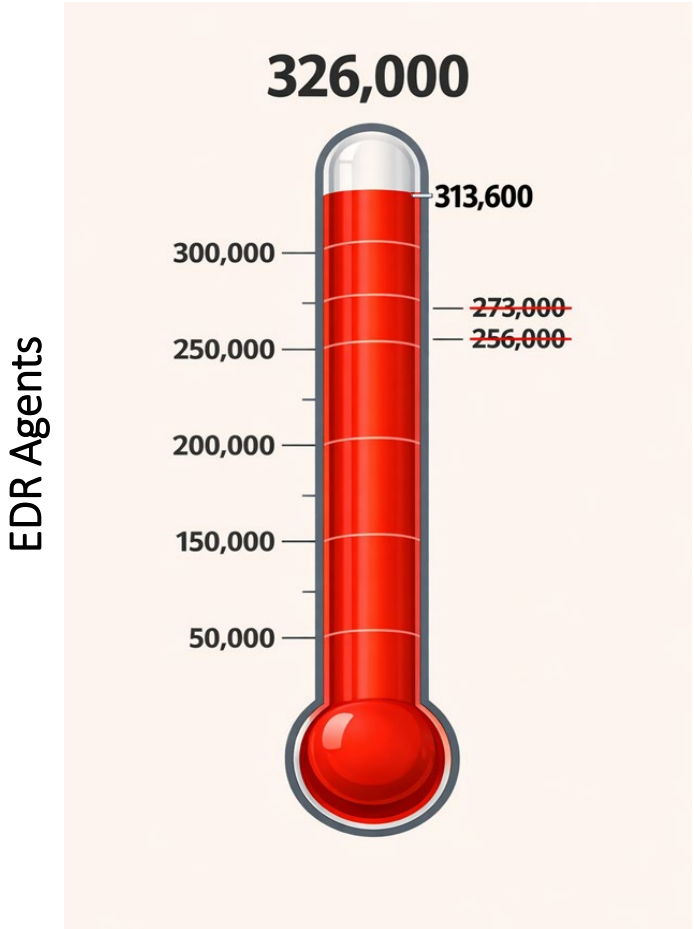


EDR Realignment

- 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 May 1, notify TEA and your ESC of your delay.

EDR – First Come, First Served



- Goal
  - $35,000,000 for EDR
  - 326,000 EDR agents deployed
- Trend
  - Jan 2026 - 256,000 agents deployed (79%)
  - Feb 2026 - 273,000 agents deployed (84%)
  - Apr 2026 – 313,567 agents deployed (96%)
- Oversubscribed Approvals
  - 433,000 Agents Approved

Texas Education Agency

Upcoming Events

Upcoming Events

- **Managed Security Services (MSS) K-12 EDR Webinar**
  - May 5, 2026, 2:30-3:30pm
  - Hosted by TEA & SAIC
  - Audience: Existing MSS K-12 EDR Customers & Schools interested in MSS EDR.
  - Registration: https://us02web.zoom.us/webinar/register/WN_wkvfXW9QQgazYqEAsWd4jQ
- **27th Annual Information Security Forum (ISF)**
  - May 20-21, 2026, Palmer Events Center, Austin
  - Hosted by DIR & TXCC
  - Audience: Government employees (state and local) and employees of K-12 and institutions of higher education. Registration is required.
  - Registration Link at: https://xcelevents.swoogo.com/isf2026attendee
- **Region One Technology Conference**
  - May 12-14, South Padre Island Convention Center
  - https://www.esc1.net/technologyconference

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.
  - Handy link to sign up for the Cybersecurity Coordinator Forum meetings.
  - Previous K-12 Cybersecurity Initiative Webinars posted on this page.
- Program Email: k12cyber@tea.texas.gov

Cybersecurity Coordinator Forum (CCF)

The **TEA Cybersecurity** team hosts a **monthly** meeting for Texas school system **Cybersecurity Coordinators, Technology Coordinators**, Education Service Center (ESC) **Cybersecurity personnel**, and other members of the community that support K-12 Cybersecurity efforts. It provides content designed to assist school systems and ESCs towards maturity in an information security program.

Next CCF: May 27, 2026 @ 11:00 AM CST

Register here:

https://t.ly/Hmimy

Please register with your school system email account.

Stay Safe & Secure

Thank you!

Questions?

Email:
k12cyber@tea.texas.gov