Cybersecurity Coordinator Forum

September 2025

Susan Bain

Cybersecurity GRC Analyst

Texas Education Agency

cybersecurity@tea.texas.gov

Cybersecurity Coordinator Forum

The **TEA Cybersecurity** team hosts a **monthly** meeting for Texas School Systems **Cybersecurity Coordinators**, **Technology Coordinators**, Education Service Center (ESC) **Cybersecurity personnel**, and other members of the community that support K12 Cybersecurity efforts. It provides content designed to assist School Systems and ESCs towards maturity in an information security program.

Register here:
https://t.ly/Hmimy

Please register with your School System email account.

TEA Leadership Update

Welcoming Our New CISO

- We are excited to announce that the Texas Education Agency has appointed a new Chief Information Security Officer (CISO), **Daniel Ramirez**, effective **August 1, 2025**. Daniel joins us from Education Service Center (ESC) 1 and brings a wealth of experience in educational cybersecurity.

- His leadership will be instrumental in advancing the K–12 Cybersecurity Initiative and ensuring the safety of our digital learning environments across Texas.

Cybersecurity Nutritional Facts

Serving Size: 1 Cybersecurity Professional

	%Daily Value*
Passion	300%
Determination	500%
Creativity	100%
Critical Thinking	1000%
Innovation	100%
Hard Work	200%
Sleep	0%
Caffeine	110%

*Percent Daily Values Are Based on Your Unique Diet

Daniel Ramirez

Chief Information Security Officer for TEA

- Started August 1, 2025

Working in IT for 28+ years

- Texas A&M Kingsville
- University of Texas Rio Grande Valley (Pan Am)
- Region One Education Service Center
- 13 of the 28+ years have been in Information Security

Security Certifications:

- Certified Information Systems Security Professional (CISSP)
- Certified Penetration Tester (SANS GIAC-GPEN) *(*not active)*

Agenda

- 89th Session Legislative Updates
- Texas K12 Cybersecurity Initiative Update
- Cybersecurity News & Advisories

89th Session Legislative Update

Legislative Update – Technology – Artificial Intelligence

- **HB 149** - Establishes comprehensive regulations for the development, deployment, and use of artificial intelligence (AI) systems in Texas, emphasizing transparency, consumer protection, ethical use, and strong enforcement mechanisms, while also fostering innovation through a regulatory sandbox and oversight by a dedicated council.

- **HB 2818** - Establishes an Artificial Intelligence Division within DIR tasked with supporting state agencies and other entities in implementing generative artificial intelligence (AI) technology.

Legislative Update – Technology – Artificial Intelligence

- **HB 3512** - establishes requirements for artificial intelligence (AI) training programs for certain employees and officials of state agencies and local governments in Texas. It amends existing statutes to integrate AI training alongside cybersecurity training.
  - School districts must ensure their cybersecurity coordinators complete both cybersecurity and AI training annually.
  - DIR will develop forms for verification and reporting.

- **SB 1964** - establishes comprehensive regulations for the use, procurement, deployment, and management of artificial intelligence (AI) systems by Texas state agencies and local governments. It also sets standards for data management and public transparency.
  - Establishes a Public Sector AI Systems Advisory Board
  - State agencies must inventory all AI systems, including heightened scrutiny systems, and report on their purpose, risk mitigation, and compliance with strategic plans.

Legislative Update – Cybersecurity & Technology

- **HB 150** - creates the Texas Cyber Command (TCC), transferring certain cybersecurity powers and duties from the Department of Information Resources (DIR) to the new agency. The TCC will be the central authority for cybersecurity prevention, response, recovery, and training for Texas governmental entities and critical infrastructure.
  - Establishes a Cybersecurity Threat Intelligence Center, Incident Response Unit, and Digital Forensics Laboratory
  - Coordinates with regional security operations centers and other agencies for exercises and response.

- **HB 1500** - continues the existence of the Texas Department of Information Resources (DIR) until September 1, 2037, and updates its governance, training, procurement, advisory committees, and reporting requirements. It also establishes new programs and clarifies DIR's role in state assistance opportunities and cybersecurity.

- **HB 3112** - amends Texas law to provide confidentiality protections for government information related to cybersecurity measures for critical infrastructure facilities. It clarifies when government bodies can hold closed meetings and what cybersecurity information is exempt from public disclosure.

Legislative Update – Cybersecurity & Technology

- **HB 5195** - aims to modernize Texas state agency websites and digital services, improving accessibility, navigation, and efficiency for users.

- **HB 5331** - addresses the enforceability of contract language in state agency and local government contracts, specifically regarding requirements for security incident notifications.
  - Declares any contract language in a cybersecurity insurance contract or other contracts that prohibits or restricts security incident notification requirements is declared void and unenforceable.

- **SB 765** - amends the Texas Government Code to make information related to fraud detection and deterrence measures confidential and exempt from public disclosure under the state's public information law.

- **HB 5196** establishes clear guidelines and requirements for telework arrangements for Texas state agency employees, aiming to provide flexibility while maintaining accountability and security.

Texas Education Agency

Texas K12 Cybersecurity Initiative

Legislative Update – K12 Cybersecurity Initiative

- We are pleased to share that the 89th Texas Legislature has **approved an additional $42 million** in funding for the **FY26/FY27 biennium (September 2025–August 2027)**, ensuring the continuation and expansion of this critical initiative.

- Remaining funds from FY24/FY25 (approximately $26M) have also been transferred forward to support ongoing efforts.

Managed Security Services (MSS)

- DIR has awarded SAIC the contract for MSS
  - As of September 1, 2025
- Was previously held by AT&T
- Transition has been transparent for all School Systems
- The MSS services under SAIC have a few minor terminology changes

Ongoing Goals – K12 Cybersecurity Initiative

- Current goals are still in effect and will be carried forward in FY26/27
  - Implement fully managed **Endpoint Detection and Response (EDR)** on School System servers and applicable staff devices.
  - Implement **Multi-Factor Authentication (MFA**) for staff email systems**.**
  - Ensure **Domain-based Message Authentication, Reporting, and Conformance (DMARC) Compliance** to enhance protection against phishing and spoofing**.**
  - Restrict **local administrator access** to minimize the risk of unauthorized system changes.
  - Complete a **Texas Cybersecurity Framework (TCF) assessment** to get a baseline of cybersecurity program and action plan for improving maturity.
  - Implement **Network Detection and Response (NDR**).
    - NDR Pilot is paused to new customers as we evaluate a more viable cost option

Fully Funded Services ($0 Cost to School Systems)

- **Fully funded services currently available for request :**
  - **Managed Endpoint Detection and Response (EDR)**
    - Requirement: student enrollment **50,000** or less, licenses up to **30%** enrollment, 30 license min.
    - Once registered, request service via Managed Security Service (MSS): MSS Portal Log In Process (texas.gov).
    - School Systems may choose between EDR vendors CrowdStrike or SentinelOne.
    - Shared (~~Standard~~) option should be most common for School Systems.
  - **Texas Cybersecurity Framework (TCF) Assessment (*aka School District Cybersecurity Assessment (SDCA)*)**
    - Requirement: First come, first served for **any** School System.
    - Once registered, request service via MSS : TX K-12 Cybersecurity Assessment Quick Start Guide
    - School Systems may choose between Small (~~Basic~~), Medium (~~Intermediate~~), or Large (~~Advanced~~) Cybersecurity Assessments.
    - May be ordered now and scheduled for any time through August 2027.
  - **Network Detection and Response (NDR) – Pilot Program Closed for FY23 - FY25**
    - NDR pilot results are being evaluated to determine inclusion for FY26 – FY27.
    - NDR vendor is Vectra.

https://tea.texas.gov/academics/learning-support-and-programs/technology-planning/sts-new-customer-information-form.docx

Program Participation - ILC

- **School Systems that have onboarded with DIR**
  - 500+ School Systems have signed the DIR InterLocal Contract (ILC) form. (~40%)

- Goal: 100% of School Systems complete a signed ILC with DIR.
- Why?
  - **Zero** Commitment to request any services
  - **Zero Cost** for any TEA K12 Cybersecurity Initiative services in scope
  - ILC process takes time to complete
    - Superintendent Signoff, Board Approval, etc.
    - Cannot provide EDR or other services until signed ILC is on file

DIR = Texas **D**epartment of **I**nformation **R**esources

ILC & STS Portal Access Process

1. School System Completes **New Customer Form,** send to DIR
   - *No signatures required*
2. DIR Receives New Customer Form and Sends School System the **Interlocal Contract (ILC)**
3. School System reviews, completes, approves, and signs ILC
   - *Requires Superintendent Signature*
4. School System sends signed ILC to DIR for processing
5. DIR reviews and approves ILC, then **STS Portal Access** Granted (to listed technical contacts on New Customer Form)
6. School System requests MSS services via STS Portal
   1. EDR
   2. TCF Assessment

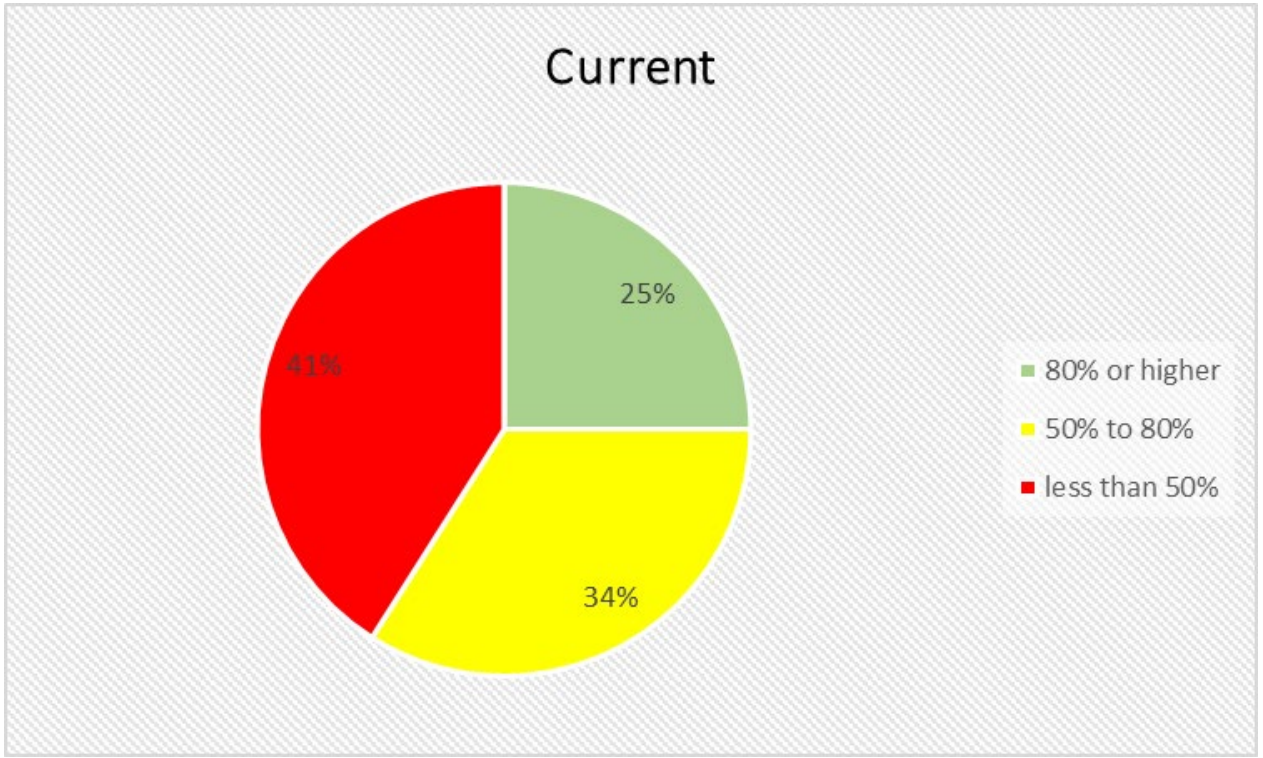
Program Participation - EDR

- **End Point Detection Response (EDR)**
  - 342 School Systems have signed up for EDR
  - Installed on 235,000 endpoints.
  - 40,600+ attacks blocked.
  - 10,500+ ransomware threats neutralized.

- ESCs tasked with assisting school systems to deploy EDR at no cost.

Program Participation - EDR Agent Deployment

K12 Cybersecurity Initiative - EDR Deployment Metrics
(Requested vs % Deployed)



Ransomware Incidents – (Feb. 2025 – August 2025)

- Six (6) Ransomware Incidents reported by Texas School Systems
  - Avg. one (1) per month, between February and August 2025
  - Only two (2) had EDR as part of the K12 Cybersecurity Initiative.
    - Had not fully deployed to all in scope systems
  - The other four (4) have now deployed EDR.

EDR In-Scope Computers

- School Systems need comprehensive EDR coverage
  1. On-Prem Servers (100%)
  2. IT Staff & Central Office Staff Computers
  3. Teacher Computers
  4. All remaining staff computers
  5. Student Lab Computers (must remain on campus)

  Start at 1 and move down list until all approved agents are deployed. If additional agents are needed for 1, 2, or 3 then submit and Add-On request when you are at ~90%.

Program Participation – TCF Assessments

- **Cybersecurity Assessments**
  - 54 School Systems have signed up; 42 completed.

SIZE	In Progress	Completed
Small	3	12
Medium	0	6
Large	9	24

  - Individual results from the assessments are kept confidential.
  - Assessments are a powerful tool that can be used to:
    - Raise awareness of School System risks and help to determine a plan of action for those risks
    - Used to communicate the risk to School System leadership team
    - Support requests for additional funding.
  - School Systems can re-assess after 12 months, after they have made improvements and mitigated findings.

TCF Assessment Sizes

FUNCTIONAL AREA	CONTROL	SMALL	MEDIUM	LARGE
IDENTIFY	Privacy and Confidentiality	X	X	X
	Data Classification	X	X	X
	Critical Information Asset Inventory	X	X	X
	Enterprise Security Policy, Standards and Guidelines	X	X	X
	Control Oversight and Safeguard Assurance		X	X
	Information Security Risk Management		X	X
	Security Oversight and Governance		X	X
	Security Compliance and Regulatory Requirements Management		X	X
	Cloud Usage and Security	X	X	X
	Security Assessment and Authorization / Technology Risk Assessments		X	X
	External Vendors and Third Party Providers	X	X	X
PROTECT	Enterprise Architecture, Roadmap and Emerging Technology			X
	Secure System Services, Acquisition and Development			X
	Security Awareness and Training	X	X	X
	Privacy Awareness and Training	X	X	X
	Cryptography		X	X
	Secure Configuration Management		X	X
	Change Management			X
	Contingency Planning			X
	Media	X	X	X
	Physical and Environmental Protection	X	X	X
	Personnel Security	X	X	X
	Third-Party Personnel Security			X
	System Configuration Hardening and Patch Management	X	X	X
	Access Control	X	X	X
	Account Management	X	X	X
	Security Systems Management	X	X	X
	Network Access and Perimeter Controls	X	X	X
	Internet Content Filtering	X	X	X
	Data Loss Prevention	X	X	X
	Identification and Authentication	X	X	X
	Spam Filtering	X	X	X
	Portable and Remote Computing	X	X	X
	System Communications Protection	X	X	X
	Information Systems Currency			X
DETECT	Vulnerability Assessment	X	X	X
	Malware Protection			X
	Security Monitoring and Event Analysis	X	X	X
	Audit Logging and Accountability			X
RESPOND	Cyber-Security Incident Response	X	X	X
	Privacy Incident Response			X
RECOVER	Disaster Recovery Procedures	X	X	X

42 Total Controls

- Small = 26 Controls
- Medium = 33 Controls
- Large = all 42 Controls

Program Participation – NDR

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

ESC Support

- Email Domain Security (SPF, DKIM, DMARC Conformance)
  - Configuration, No Cost
- Multi-Factor Authentication on ALL employee email accounts. (Microsoft 365 & Google Workspace)
  - Employee Awareness, Configuration, No Cost
- Restrict Local Admin Privileges
  - Employee Awareness, Configuration, No Cost

New Goals – K12 Cybersecurity Initiative

- New goals are being developed and considered for FY26/27
- Recommendations have been gathered from TEA CISO and TASI
- Survey will go out in late September to School Systems and ESCs asking for feedback on additional needs
  - Please be sure to complete the survey once you receive it. Your responses are essential for TEA to accurately assess the current impact and understand the cybersecurity needs of our school systems.

K12 Cybersecurity Initiative Website

- Has been recently updated!
- https://tea.texas.gov/academics/learning-support-and-programs/technology-planning/k-12-cybersecurity-initiative
  - Steps to onboarding School Systems to DIR STS portal can be accessed on this page
  - Updates about the program
  - Frequently asked questions about the program
  - Handy link to sign-up for the Cybersecurity Coordinator Forum meetings
  - Previous K12 Cybersecurity Initiative Webinars posted on this page

K12 Cybersecurity Contacts

- SAIC
  - L_TXDIR_MSS_EDR@saic.com (EDR Support)
  - L_TXDIR_MSS_SOC@saic.com (Security Team) *
  - Toll Free Hotline 1.800.536.9706 (MSS SOC Team) *
- DIR
  - cirt@dir.texas.gov (cybersecurity incident response team) *
  - Toll Free Hotline (877) DIR-CISO (1.800.347.2476) *
- TEA
  - cybersecurity@tea.texas.gov
- ESC
  - Request from your ESC

Other Operational Services Requests

- non-incident, operational requests
- quickly receive help for non-incident requests, such as user provisioning and removal, console login issues, agent installations, uninstalling agents, agent upgrades, whitelisting software, etc.
- please begin the **provide brief 40-character summary** field with "MSS -" followed by your summary description. This assures that the request is correctly routed to SAIC.
- https://txdir.servicenowservices.com/sp?id=sc_cat_item&sys_id=9d4bc3961318ab804210f65ed144b062&sysparm_category=9955beb91bfed054a04b74c8dc4bcbd7

Update your School System Contacts

- Update AskTED
  - Technology Coordinator & Cybersecurity Coordinator
  - *Request assistance from your TED Administrator to update AskTED*
- Update contact info with your ESC
  - Provide a primary and a backup contact
- Update contact info for STS Portal Access
  - Email terese.shade@dir.texas.gov if you have lost access
- Update contact info with SAIC SOC Team *
- Update all the above when Technology or Cybersecurity Coordinators change

Texas Education Agency

Cybersecurity News & Advisories

TX-ISAO

The Texas Information Sharing & Analysis Organization (TX-ISAO) is open to all organizations in Texas to include K-12.

- Established by DIR to enable Texas entities to share cybersecurity threat intelligence, best practices and remediation strategies.

ACTION: Please sign up for mailing list at the link below.

https://dir.texas.gov/txisao

Recent Cyber Incidents in the News

- Tenable Data Breach – September 8, 2025
  - Part of a broader attack on Salesforce and Salesloft Drift
  - Unauthorized access to customer data stored in Salesforce
  - https://www.tenable.com/blog/tenable-response-to-salesforce-and-salesloft-drift-incident
- TransUnion Data Breach – August 2025
  - 4.4 million individuals affected
  - Data stolen from Salesforce account
  - https://www.bleepingcomputer.com/news/security/transunion-suffers-data-breach-impacting-over-44-million-people/

Recent Cyber Incidents in the News (cont.)

- Farmers Insurance Breach – August 2025
  - 1.1 million customers impacted
  - Breach linked to Salesforce vulnerabilities
  - https://www.bleepingcomputer.com/news/security/farmers-insurance-data-breach-impacts-11m-people-after-salesforce-attack/

- Jaguar Land Rover Cyberattack – September 2, 2025
  - Production halted due to a cyberattack affecting internal systems
  - Unclear if customer or supplier data was compromised
  - https://www.bleepingcomputer.com/news/security/jaguar-land-rover-extends-shutdown-after-cyberattack-by-another-week/

Recent Cyber Incidents in the News (cont.)

- Google Salesforce CRM Breach – August 6, 2025
  - Social engineering attack via fake IT calls led to data theft across multiple companies.
  - https://www.bleepingcomputer.com/news/security/google-suffers-data-breach-in-ongoing-salesforce-data-theft-attacks/
- Cisco Vishing Attack – August 5, 2025
  - Employee tricked via voice phishing, exposing sensitive user data.
  - https://techcrunch.com/2025/08/05/hacker-used-a-voice-phishing-attack-to-steal-cisco-customers-personal-information/

- Cybersecurity Coordinator Forum – Save The Dates!
  - October 22, 2025 @ 11:00 AM CDT
  - ~~November 26, 2025~~
  - ~~December 24, 2025~~
  - January 28, 2026 @ 11:00 AM CST

- What would you like included in the next CCF?
  - Email us: cybersecurity@tea.texas.gov

Stay Safe & Secure

Thank you!

Questions?

Email :

cybersecurity@tea.texas.gov