Cybersecurity Coordinator Forum

May 2026

Daniel Ramirez

Chief Information Security Officer

Texas Education Agency

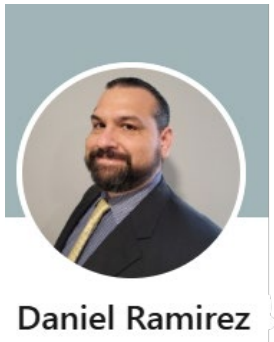
cybersecurity@tea.texas.gov

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.

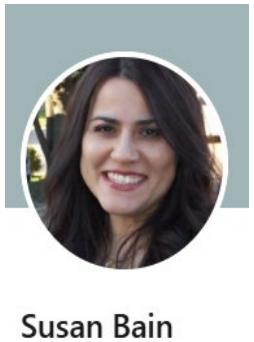
The TEA Team

- 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 - Sr. Cybersecurity Operations Analyst

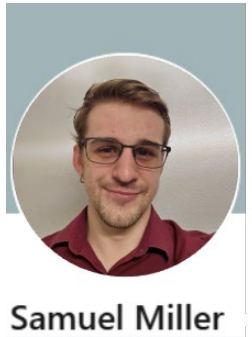

Daniel Ramirez


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
- Invite co-workers and peers to join!

Agenda

- Introductions & Housekeeping – Daniel Ramirez
- Legislative Updates – Daniel Ramirez
- Cybersecurity Advisories – Daniel Ramirez
- Emerging Trends – Myles Muchineuta
- K-12 Cybersecurity Initiative Updates – Daniel Ramirez & Brent Baker
- 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)

Texas Education Agency

Cybersecurity Advisories

Canvas (Instructure) Security Incident - Overview

Incident Overview

- Cybersecurity incident impacting Canvas LMS reported in late April to early May 2026
- Activity attributed to the ShinyHunters threat actor group known for large-scale data exfiltration
- Exposure of user data including names, email addresses, student IDs, and platform messages
- No indication that passwords, financial data, or government identifiers were compromised
- Impacted organizations began receiving notifications starting May 5, 2026
- Official Instructure updates: https://www.instructure.com/incident_update

Canvas (Instructure) Security Incident - Risks

Risks and Considerations

- Exposure of contact and communication data increases risk of phishing and impersonation attempts
- Threat actors often leverage compromised data for follow-on social engineering activity
- Potential risk from reused passwords across systems (Canvas, email, network, personal accounts)
- Third-party integrations (Learning Tools Interoperability (LTI) apps) may serve as additional attack vectors
- Organizations should closely monitor communications from Instructure and assess internal impact

Canvas (Instructure) Security Incident - Recommendations

Recommendations

- Force password resets for administrative and impacted user accounts
- Require unique passwords across all systems and accounts
- Enforce multi-factor authentication (MFA), especially for privileged users
- Review and audit third-party integrations within Canvas (LTI apps)
- Monitor account activity and communications for suspicious behavior
- If your organization detects malicious activity involving its Canvas LMS environment, please report it to **Texas Cyber Command** immediately through the TXCC Incident Response Hotline at **(877) 347-2476**.

TEA Learn (Canvas Hosted)

- **Current Status**
  - TEA Learn instance (hosted on Canvas) was reviewed following the recent Canvas security incident
  - No TEA data exposure identified
  - Environment has been validated and cleared for continued use
  - TEA implemented additional safeguards to protect data and connections
- **Recommended Actions for School Systems**
  - Require / encourage password changes for all TEA Learn users
  - Increase phishing & social engineering awareness
    - Remind staff and students to:
      - Not click on unknown links
      - Verify unexpected requests with IT Staff
  - Reinforce credential hygiene
    - Never reuse school account **passwords** on:
      - Personal websites
      - Third-party or non-school systems (including TEA Learn, TEAL, etc.)
    - Encourage use of separate credentials for personal accounts
- **Key Reminder**
  - While TEA Learn remains secure, the broader incident increases risk of targeted phishing using known school-related data

Follett Software – Potential Data Breach (May 2026)

- **What We Know**
  - A ransomware group (ShinyHunters) claimed a breach of Follett Software LLC on April 30, 2026
  - Alleged access to ~4M Salesforce records containing PII and internal data
- **Status**
  - Unverified claim — no confirmed breach or data leak
  - No public statement or guidance from Follett to customers
  - No confirmed impact to specific school systems
- **Potential Risk**
  - Follett software is widely used by some districts for library, content and resource management.
  - If validated, could involve student/staff data or system integrations
- **Recommended Precautions (At This Time)**
  - Review Follett system integrations (SSO, API access)
  - Ensure MFA and credential hygiene for staff accounts
  - Monitor for unusual activity tied to Follett platforms
- **Bottom Line**
  - Treat as a credible but unconfirmed third-party risk event
  - Maintain heightened vigilance until further verified information is available

McGraw Hill Data Breach (April 2026)

- **What We Know**
  - Data exposure tied to a Salesforce misconfiguration (not a core systems compromise)
  - ~13.5 million user records confirmed exposed; dataset >100GB publicly leaked
  - Data includes: emails, names, phone numbers, physical addresses (inconsistent across records)
  - Attributed to ShinyHunters extortion group (“pay-or-leak”)
- **Status**
  - Data has been publicly released on criminal forums
  - McGraw Hill states internal systems, courseware, and grading platforms were not impacted
  - No evidence of SSNs, financial data, or credentials exposed (based on current reporting)
- **Potential Risk to Schools**
  - Increased phishing/spear-phishing targeting students, staff, and administrators
  - Social engineering using trusted education context (McGraw Hill references)
  - Risk of account takeover attempts leveraging reused credentials
- **Recommended Precautions**
  - Alert staff to heightened phishing risk tied to education vendors
  - Emphasize verification of vendor communications (email/domain scrutiny)
  - Enforce/review MFA on all staff- and student-facing systems
  - Review third-party/SaaS access controls and data exposure settings

McGraw Hill Data Breach (April 2026) - *continued*

- **Bottom Line**
  - This was a large-scale SaaS misconfiguration exposure, not a direct breach of school systems—but the public release of millions of education-related contact records significantly increases phishing and social engineering risk for districts.

Guidance on TXCC Network Blocking of Prohibited Technology

- **Background**
  - Texas Cyber Command (TXCC) implemented network blocking controls targeting high-risk infrastructure
  - This included high-risk:
    - IP addresses & CIDR (classless inter-domain routing) ranges
    - Domains (including wildcards)
    - Autonomous system numbers (ASNs)
- **Key Clarification**
  - Lenovo and Motorola devices are NOT listed in the prohibited hardware list
  - Action is network-level blocking only (not a device ban)
  - Blocking may impact services tied to affected infrastructure
- **What This Means for School Systems**
  - No communicated requirement to:
    - Remove Lenovo or Motorola devices
    - Replace existing hardware
  - Focus is on risk reduction via network connectivity controls, not asset removal

Required Actions & Strategic Guidance

- **Immediate Actions**
  - Implement TXCC-provided indicators (IPs, domains, ASNs)
  - Monitor for device functionality issues, updates/patching disruptions, and vendor service impacts
- **Procurement & Risk Management**
  - Avoid single-vendor dependency
  - Evaluate vendor risk (geopolitical & supply chain)
  - Maintain flexibility in contracts where feasible
- **Operational Guidance**
  - Continue planned procurements with due diligence
  - Do NOT act on speculation regarding future bans
  - Rely only on official state guidance
    - https://dir.texas.gov/information-security/covered-applications-and-prohibited-technologies
- **Strategic Recommendation**
  - Strengthen vendor risk management:
    - Identify critical dependencies
    - Develop contingency plans
    - Improve visibility into vendor connectivity

Texas Education Agency

Emerging Threats

Scattered Lapsus$ ShinyHunters - Data Theft and Extortion Campaign

- The FBI has issued a FLASH (FBI Liaison Alert System) report on recent activity conducted by a combination of multiple known cybercriminal groups (AKA Scattered Lapsus$ ShinyHunters (SLSH)). This Hacker Alliance blends tactics from multiple known cybercriminal groups and focuses on:
  - Identity compromise (rather than malware)
  - Data theft from SaaS/cloud platforms
  - Extortion and real-world harassment

- The activity is particularly dangerous because it:
  - Uses legitimate credentials
  - Exploits trusted relationships (vendors, integrations)
  - Targets enterprise SaaS and IAM environments

Source: The Federal Bureau of Investigation (FBI) Flash

Date: May 2026 | FLASH-20260508-001

Scattered Lapsus$ ShinyHunters - Data Theft and Extortion Campaign

Overall Tactics:

- Primary attack vector: Social engineering, especially voice phishing (vishing)
- Primary target: Identity systems (IAM), CRM platforms, and cloud data
- Goal: Large-scale data exfiltration + extortion
- Unique trait: Often no malware is used—attacks occur entirely through valid access
- Escalation: Includes harassment, swatting, and DDoS to pressure victims

Scattered Lapsus$ ShinyHunters - Data Theft and Extortion Campaign

How the Attack Works (At a High Level)

1. Initial Access
   - Conduct vishing attacks impersonating IT/help desk
   - Direct users to fake login portals
   - Induce: MFA approvals & credential resets
2. Credential Abuse & Access Expansion
   - Use compromised credentials to:
     - Access IAM platforms
     - Pivot into multiple enterprise systems
     - Expand access without triggering traditional alerts
3. Persistence & Obfuscation
   - Use: VPNs & residential proxies
   - Blend activity with normal user behavior
4. Data Access & Exfiltration
   - Operate directly in SaaS platforms
   - Use APIs to:
     - Enumerate data & extract data in bulk
   - No need to deploy malware

Scattered Lapsus$ ShinyHunters - Data Theft and Extortion Campaign

How the Attack Works (continued)

5. Third-Party Pivoting (Critical Risk)

- Compromise vendors (e.g., CRM integrations, MSPs)
- Steal stored credentials/tokens
- Pivot into downstream customer environments

6. Extortion & Coercion

- Victims receive:
  - Email from ShinyHunters-branded accounts
  - Payment demand (typically cryptocurrency within ~72 hours)
- Escalation tactics include:
  - Phone/SMS harassment
  - Contacting employee family members
  - Swatting incidents
  - DDoS attacks
- Data is published on Tor leak sites if unpaid

Scattered Lapsus$ ShinyHunters - Data Theft and Extortion Campaign

What to Watch For

Authentication Anomalies

- Login from new or proxy-based IPs
- MFA fatigue or unusual approval behavior

Data Activity

- Immediate high-volume API activity after login
- Bulk data exports

User Behavior Mismatch

- Sudden browser/device changes
- Inconsistent user-agent strings

Vendor Activity

- Third-party accounts accessing:
  - Multiple systems
  - Large datasets outside normal patterns

Scattered Lapsus$ ShinyHunters - Data Theft and Extortion Campaign

- Mitigation Strategy

  Identity Security (Critical Control Layer)

  - Enforce phishing-resistant MFA (FIDO2, hardware tokens)
  - Apply conditional access policiesa
  - Restrict access from anonymized networks

  Help Desk Hardening

  - Require multi-channel identity verification
  - **Do NOT allow**:
    - Password resets via phone alone
    - MFA changes without validation

  SaaS & API Monitoring

  - Enable detailed logging
  - Alert on: Bulk data access and abnormal API usage
  - Enforce least privilege

Scattered Lapsus$ ShinyHunters - Data Theft and Extortion Campaign

- Mitigation Strategy (Continued)

  Third-Party Risk Management
  - Audit vendor access
  - Monitor vendor authentication patterns
  - Rotate credentials and API keys regularly

  Organizational Readiness
  - Train users to recognize phishing/vishing
  - Monitor: API usage, IAM logs, Browser session anomalies
  - Review all CRM/cloud integrations

More information can be found below: RSA Archer GRC Platform

Scattered Lapsus$ ShinyHunters - Data Theft and Extortion Campaign

- The FBI assesses this as a high-impact threat because:
  - It exploits identity rather than endpoints
  - Uses trusted relationships (vendors)
  - Enables silent, large-scale data exfiltration
  - Combines cyber intrusion with real-world coercion tactics
- Organizations most at risk are:
  - Those with exposed IAM systems
  - Heavy SaaS/cloud usage
  - Extensive third-party integrations
  - Access to sensitive customer/enterprise data

Critical Apache ActiveMQ Vulnerability

- A critical vulnerability has been identified in Apache ActiveMQ. The platform's web console exposes a management interface that, by default, allows certain powerful actions to be performed.
- Because of how the system handles and validates incoming requests, an attacker with access to the console can abuse this weakness to load unauthorized configuration files. This process causes the server to run unintended programs, giving the attacker the ability to execute commands on the system that hosts ActiveMQ.
- Impacted Versions:
  - Apache ActiveMQ 5.x — any version before 5.19.4
  - Apache ActiveMQ 6.x — any version before 6.2.3

Source: Texas Department of Information Resources (DIR)

Date: April 2026 | PUB0006860

Critical Apache ActiveMQ Vulnerability

- **Impact:** An authenticated attacker can achieve complete remote code execution on the ActiveMQ broker JVM. This allows attackers to execute arbitrary commands with the privileges of the broker process, potentially leading to complete broker compromise, data theft, lateral movement within the network, and service disruption. Active exploitation is occurring in the wild with public proof-of-concept code available.

- **Mitigation:** Immediately upgrade Apache ActiveMQ to patched versions (5.19.4+ or 6.2.3+). Restrict network access to the Jolokia endpoint at /api/jolokia/ to authorized users and systems only. Implement authentication controls and network segmentation to limit access to the ActiveMQ web console. Monitor for suspicious requests to the Jolokia endpoint and unusual process execution from the ActiveMQ JVM. Review ActiveMQ MBean policies to ensure only necessary operations are permitted.
- Evaluate your environment for any systems running older, unpatched releases of Apache ActiveMQ and take immediate actions to remediate.

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)**
  - 400 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.

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

The TASI Office Team

Technology Alliance for Statewide Initiatives

- Lea Castillo – TASI Director
- Brent Baker, CISSP, CISA – TASI Information Security Coordinator
- Emilio Estevez - TASI Projects and Grants Project Coordinator

Lea Castillo

Brent Baker

Emilio Estevez

ESC Support for the TEA K-12 Cybersecurity Initiative

- **Technology Alliance for Statewide Initiatives (TASI)**
  - Works with your ESC to provide you with information and assistance necessary for participating in all K-12 Cybersecurity Initiative services at no cost to schools.
  - Provides continued, direct support for implementation of Multi-Factor Authentication (MFA), Email Security Protocol (ESP/DMARC*), and Limited Local Administrator Access (LLA).
  - Offers a range of new K-12 Cybersecurity Initiative services (below).
- **New**: Security Awareness Training and Phishing Simulations (Infosec IQ)
  - Available **immediately** to **all** schools, regardless of size
  - The sole product currently available through TASI is **Infosec IQ**
- **Coming Soon:** Cloud Hardening Guides (Google and M365)
  - Your ESC will contact you with information June 1st
  - Based on Center for Internet Security (CIS) cloud benchmark guides
  - Delivers improvement in many control areas (MFA, ESP, etc.)
- **Coming September 1st**: Software Deployment Solution
  - For rollout of EDR agents and other software packages
  - Information will come from your ESC this summer

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

ESC Support for the TEA K-12 Cybersecurity Initiative

ESC 1 Homar Venecia hvenecia@esc1.net (956) 222-6578	**ESC 6** Robert Wyatt rwyatt@esc6.net (936) 435-8276	**ESC 11** Cole Wolsch cwolsch@esc11.net (817) 740-3696	**ESC 16** Jandi Tyson jandi.tyson@esc16.net (806) 677-5269
ESC 2 Marco Mendez marco.mendez@esc2.us (361) 561-8449	**ESC 7** Steve Vaughn steve.vaughn@esc7.net (903) 988-6922	**ESC 12** Keith Macik keith.macik@esc12.net (254) 297-1264	**ESC 17** Kyle Plumlee kplumlee@esc17.net (806) 281-5851
ESC 3 Jeff Harris jharris@esc3.net (361) 573-0731 x 1261	**ESC 8** Rodney White rwhite@reg8.net (903) 575-2788	**ESC 13** Kevin Wier kevin.wier@esc13.txed.net (512) 919-5209	**ESC 18** Bowen Pugh bowen.pugh@esc18.net (432) 561-4321
ESC 4 Tim Jing tim.jing@esc4.net (713) 744-6847	**ESC 9** Michael Chapman Jr. michael.chapmanjr@esc9.net (940) 322-6928	**ESC 14** Kevin Hill khill@esc14.net (325) 675-8600	**ESC 19** Nancy Cruz nchardin@esc19.net (915) 780-5337
ESC 5 Jerry Wilson jwilson@esc5.net (409) 951-1866	**ESC 10** Seth Patterson seth.patterson@region10.org (972) 348-1162	**ESC 15** Randon Lance randon.lance@esc15.net (325) 481-4081	**ESC 20** Dale Harville dale.harville@esc20.net (210) 370-5740

Email Security Service - New Service Available

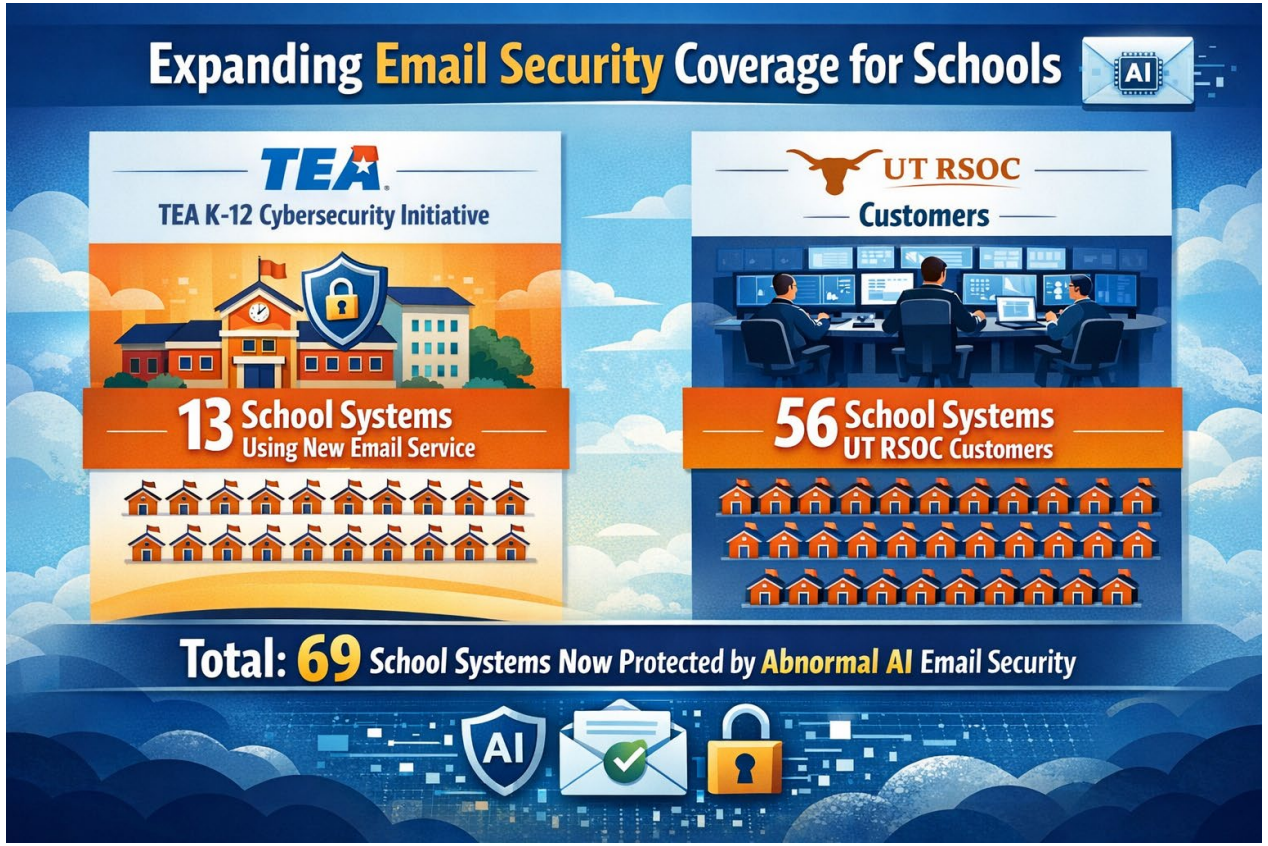
- Email Security Service available now
- Partnership with UT-RSOC using their existing email security service, Abnormal AI (previously called Abnormal Security)
- No cost to schools: all schools are eligible
- Must complete
  - TEA Pre-registration Survey (only one survey per school system)
  - UT-RSOC interlocal contract (ILC)
- Purpose of Pre-registration Survey
  - If your school is interested, we want to know your readiness and your target 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 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

Email Security Initiative Service

- 13 schools are in the approved queue.
- Off to a great start with this new initiative service
- First come, first served
- Steps:
  - Complete UT RSOC ILC
  - Submit pre-registration to TEA



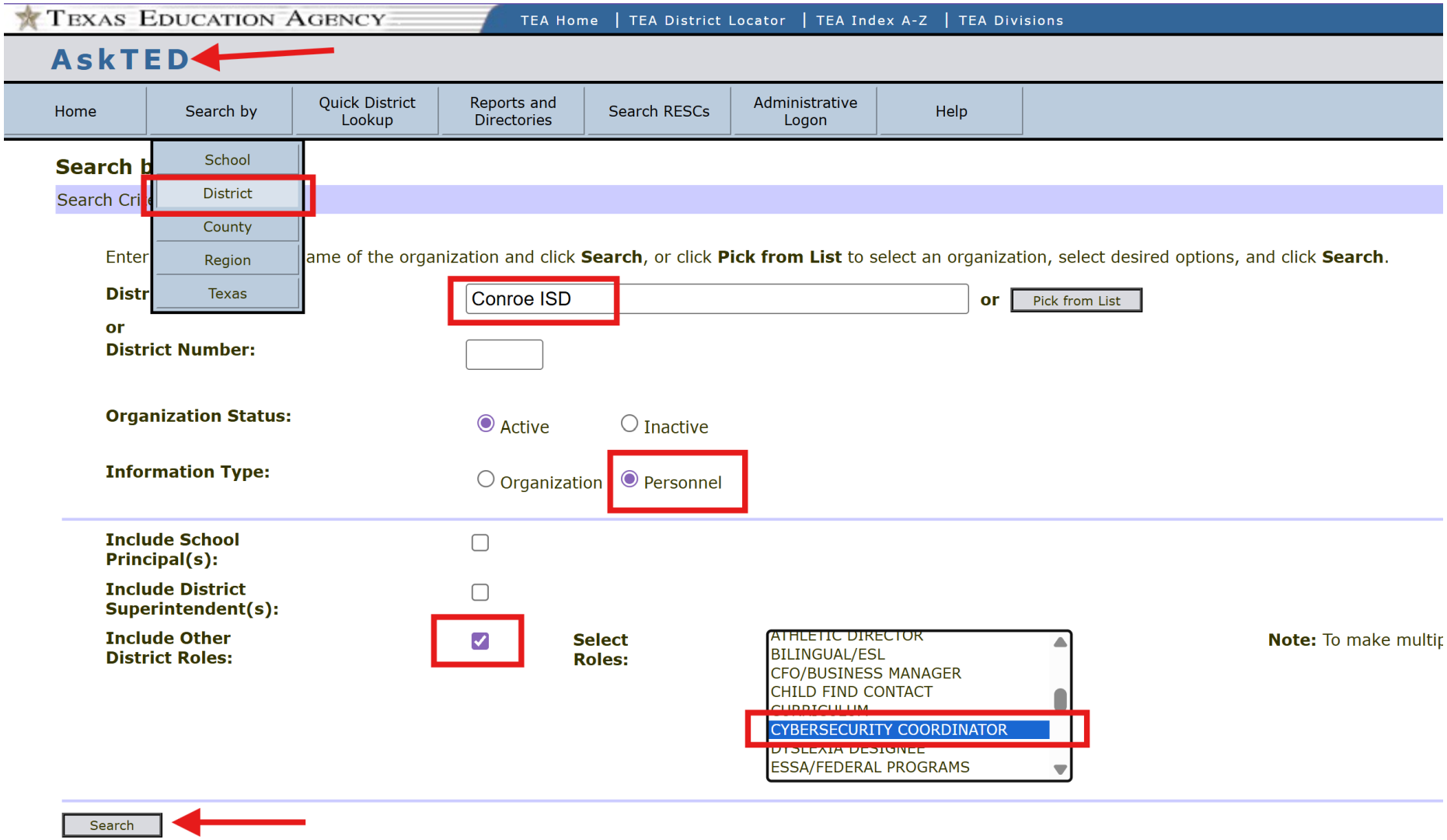
Texas Education Agency

Other Helpful Information

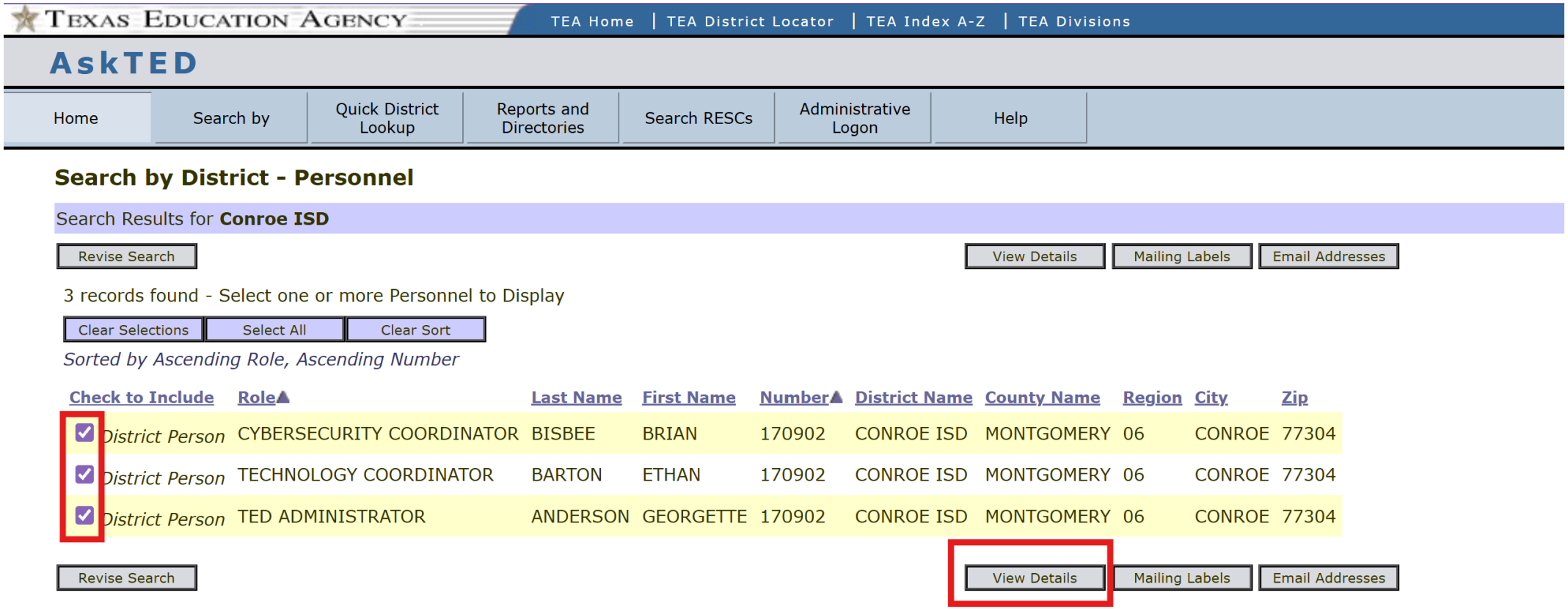
AskTED Updates

- 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).

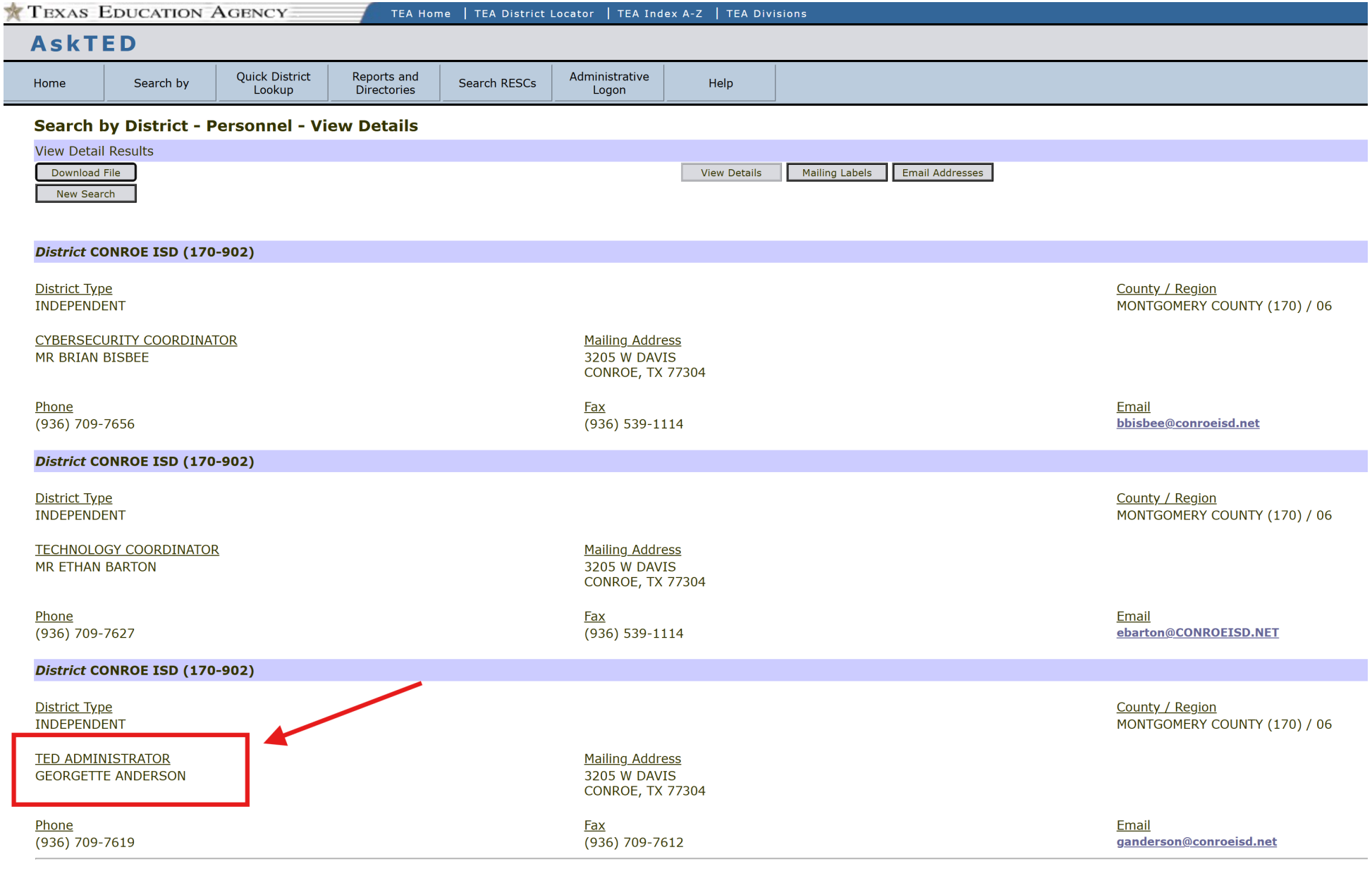
AskTED Updates



AskTED Updates



AskTED Updates



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 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

County / Region
MONTGOMERY COUNTY (170) / 06

CYBERSECURITY COORDINATOR
MR BRIAN BISBEE

Mailing Address
3205 W DAVIS
CONROE, TX 77304

Phone
(936) 709-7656

Fax
(936) 539-1114

Email
bbisbee@conroeisd.net

***District* CONROE ISD (170-902)**

District Type
INDEPENDENT

County / Region
MONTGOMERY COUNTY (170) / 06

TECHNOLOGY COORDINATOR
MR ETHAN BARTON

Mailing Address
3205 W DAVIS
CONROE, TX 77304

Phone
(936) 709-7627

Fax
(936) 539-1114

Email
ebarton@CONROEISD.NET

***District* CONROE ISD (170-902)**

District Type
INDEPENDENT

County / Region
MONTGOMERY COUNTY (170) / 06

TED ADMINISTRATOR
GEORGETTE ANDERSON

Mailing Address
3205 W DAVIS
CONROE, TX 77304

Phone
(936) 709-7619

Fax
(936) 709-7612

Email
ganderson@conroeisd.net

Texas Education Agency

Upcoming Events

Upcoming Events

- **June Cybersecurity Coordinator Forum (CCF)**
  - June 24, 2026, 11:00am
  - Hosted by TEA
  - Audience: K-12 Cybersecurity Coordinators & Technology Coordinators
  - Registration: https://t.ly/Hmimy

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

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