Texas Education Agency

Cybersecurity Coordinator Forum

Todd Pauley, CISSP

Deputy CISO/Cybersecurity Coordinator

Texas Education Agency

todd.pauley@tea.texas.gov

April 26, 2023

Cybersecurity Coordinator Forum

The TEA **Information Security** team hosts a monthly meeting for **Texas LEA Cybersecurity Coordinators**, **ESC Cybersecurity personnel**, and other members of the community that support K12 Cybersecurity efforts. It provides content designed to assist LEAs and ESCs towards maturity in an information security program.

Register here with your LEA email address:

https://attendee.gotowebinar.com/register/8234183618339320587

Agenda

- Cybersecurity Announcements
  - TxISAO (Texas Information Sharing & Analysis Organization)
  - MS-ISAC Poster Contest Winners
  - Cybersecurity Advisories
  - CISA Known Exploited Vulnerabilities
- Legislative Updates
- Texas K12 Cybersecurity Program Preparation

  Melinda Dade – Chief Information Security Officer (TEA)

Texas Education Agency

TxISAO

TxISAO

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

https://dir.texas.gov/txisao

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

MS-ISAC Poster Contest Winners

Kids in Cyber Poster Contest Winners!

Artwork from SD, TX, NY, MS

- Faith, Grade 11, VA
- Maliyah, Grade 7, SD
- Michael, Grade 10, TX
- Deangelo, Grade 5, TX
- Jax, Grade 4, MS
- Livian, Grade 12, IA
- Sahana, Grade 3, NY
- Victoria, Grade 5, TX
- Rosalind, Grade 11, VA
- Isaac, Grade 2, NY

MS-ISAC Poster Contest Winners

MS-ISAC
EI-ISAC

Contest Winners Across the States

Illustrating topics never too early to learn

MS-ISAC

Membership Overview

The Multi-State Information Sharing and Analysis Center (MS-ISAC), is part of the nonprofit Center for Internet Security (CIS). The MS-ISAC is a voluntary community focused on improving cybersecurity for State, Local, Tribal and Territorial (SLTT) governments. The MS-ISAC started in 2004. Since then we have built and nurtured an environment of collaboration and information sharing. The U.S. Department of Homeland Security (DHS) has designated the MS-ISAC as its key cybersecurity resource for State, Local Tribal and Territorial governments, including Chief Information Security Officers, Homeland Security Advisors and Fusion Centers.

There is no cost to join **the MS-ISAC, and membership is open to all SLTT government entities**. The only requirement is the completion of a membership agreement, which outlines member's responsibilities to protect information that is shared.

https://learn.cisecurity.org/ms-isac-registration

Texas Education Agency MS-ISAC

Benefits of MS-ISAC Membership

No Cost Benefits To You

- 24×7×365 Security Operations Center (SOC)
- Passive IP & Domain Monitoring
- Malicious Domain Blocking & Reporting (MDBR)
- Cybersecurity exercises
- Cybersecurity advisories
- Cyber event notifications
- Education and awareness materials
- CIS SecureSuite® Membership
- Incident response resources
- Malicious Code Analysis Platform (MCAP)
- Monthly newsletters, webinars and threat briefings
- Homeland Security Information Network (HSIN) access, including portals for communication and document sharing
- Real-Time Intelligence Sharing
- Nationwide Cybersecurity Review (NCSR)
- Discounts on training
- Vulnerability assessment services

https://learn.cisecurity.org/ms-isac-registration

Cybersecurity Advisories

Vidar Command and Control (C2)

Issue:

- In March 2023, five US IP addresses on networks associated with the Communication and Education Sectors sent a beacon to Vidar malware command and control node.

Action Items:

- See IOCs contained in the DHS bulletin in the ‘Handouts’ section.

Cybersecurity Advisories

Google Chrome Zero Day (x2)

Issue:

- Vulnerability in a memory allocation engine. This has been exploited in the wild to take control and inject malicious instructions.

Mitigation:

- Upgrade to version 112.0.5615.137 or later.

https://www.securityweek.com/google-patches-second-chrome-zero-day-vulnerability-of-2023/

Known Exploited Vulnerabilities

CISA's Known Exploited Vulnerabilities (KEV)

https://www.cisa.gov/known-exploited-vulnerabilities-catalog

- Focus on publicly accessible applications and websites.

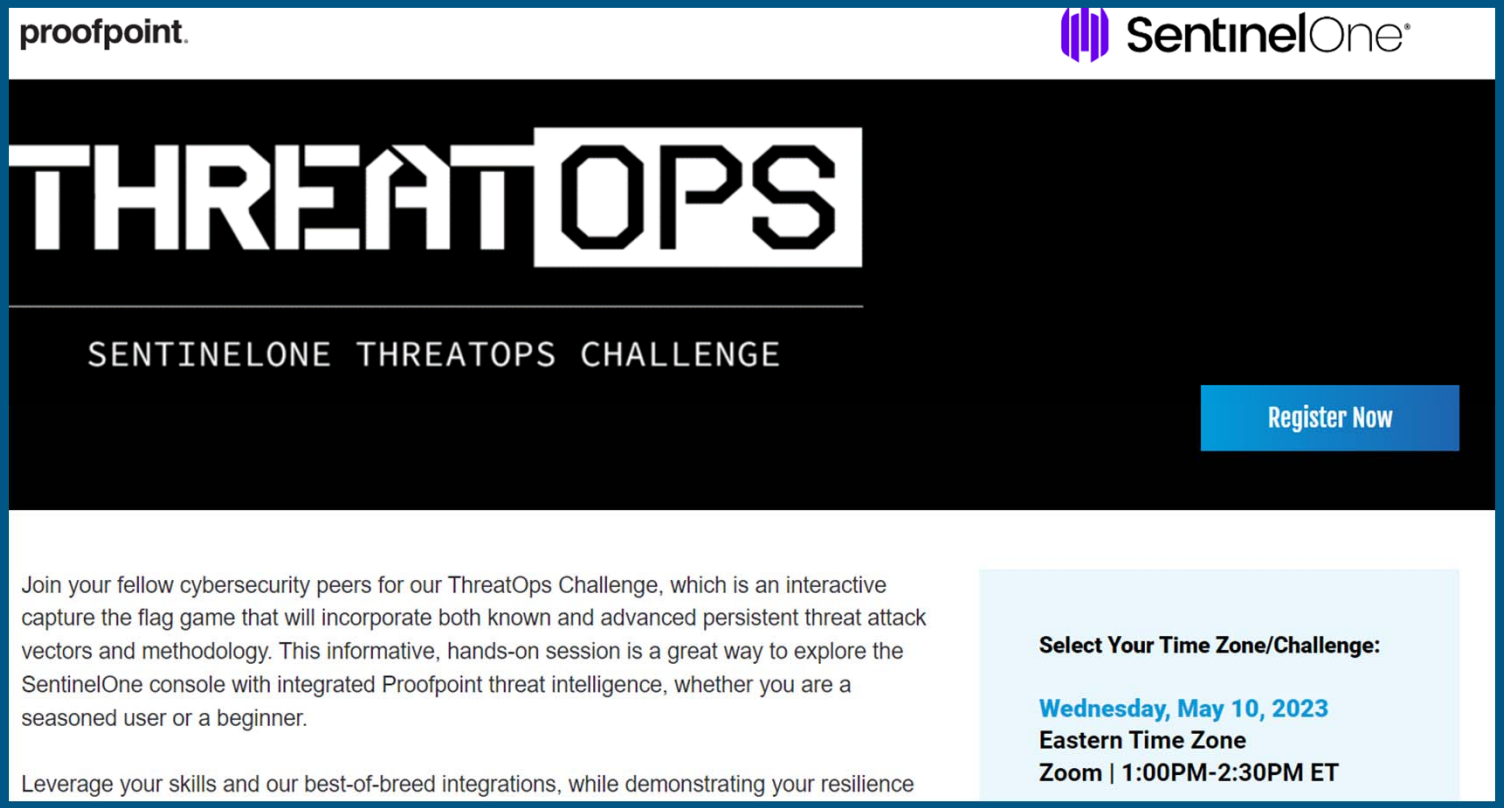
  (see download in 'Handouts')

- Sign up for the notifications of Known Exploited Vulnerabilities.

- Free on-line version with added threat intelligent information.

https://nucleussec.com/cisa-kev/

ThreatOps Challenge



https://go.proofpoint.com/ThreatOpsChallengeMay10.html?rbn=S1

Texas Education Agency

Legislative Updates

Legislative Updates

88th Legislative Session

140 days of lawmaking

- Jan. 10th : The regular session of the 88th Texas Legislature convened.
- March 10th : Deadline to propose any additional bills to the already 1,600 amassed before the session began.
- May 29th : Session adjournment (sine die).
- June 18th : Post-session deadline for the governor to sign or veto legislation.
- September 1st : Date most passed bills take effect (FY 2024).
- DIR's Cybersecurity Bill Tracking: https://dir.texas.gov/technology-legislation?id=31

Legislative Updates

Passed the Senate.
Progressing through the House.

HB 712 / SB 271

Local Governments Security Incident Procedures

- Updates Government Code 2054.1125 to include local governments in reporting requirements that previously only applied to state agencies.

- Notify DIR and State of Texas CISO within 48 hours of discovery and detailed account within 10 days after eradication.

"Security incident" means the actual or suspected unauthorized access, disclosure, exposure, modification, or destruction of sensitive personal information, confidential information, or other information the disclosure of which is regulated by law, including:

(A) a breach or suspected breach of system security as defined by Section 521.053, Business & Commerce Code; and

(B) the introduction of ransomware, as defined by Section 33.023, Penal Code, into a computer, computer network, or computer system.

Legislative Updates

Passed the Senate.
Progressing through the House.

HB 1660 / SB 768

Reporting Data Breach Information to the Attorney General

Reporting on data breaches involving 250 Texans:

- Changes timeframe from 60 days to as soon as practicable but no later than 30 days after discovery.

Legislative Updates

Passed the Senate.
Received favorably by the House.

SB 1893 / HB 3289

Relating to prohibiting the use of certain social media applications and services on devices owned or leased by governmental entities.

- Would ban TikTok and any other applications my by its parent company, ByteDance.
- Would ban any applications declared by executive order of the governor.

Legislative Updates

Progressing through both chambers.

HB 984 / SB 782
Chief Privacy Officer in the Department of Information Resources

(c) The chief privacy officer may assist local governments and the public with data privacy and protection concerns by:

(1) developing and promoting the dissemination of best practices for the collection and storage of personally identifiable information, including establishing and conducting training programs for local governments; and

(2) educating consumers about the use of personally identifiable information on mobile and digital networks and measures that can help protect the user ’s data.

Legislative Updates

Progressing through the House.

HB 2673

Relating to requirements for the use and transfer of electronic devices to students by a public school.

- The agency shall adopt standards for permissible electronic devices and software applications used by a school district or open-enrollment charter school.
    - Minimize data collection through applications.
    - Ensure parental consent.
    - Protect mental health information.
    - Ensure parents are partners in cybersecurity.
    - Mandatory down-time for devices.
- Internet filter that prohibits pornographic or obscene materials or applications including from unsolicited pop-ups, installations, and downloads.

Legislative Updates

- **HB 1659 Cybersecurity Trainings for LEAs**
  Has been stuck in committee for a few weeks.
- **SB 1205 Relating to the modernization of information technology of state agencies and certain local governments.** (ISDs to use .gov top level domain.)
  Referred to Business and Commerce
- **SB 928 Relating to the protection of personally identifiable student information and the use of covered information by an operator or educational entity; authorizing a civil and administrative penalty.** (Biometric Data)
  Has not had any movement since TEA made comments.
- **HB 2790 Relating to access to social media and social networking websites on public school campuses.**
  Hasn't had any movement since mid March.
- **SB 2377 Relating to Homeland Security** (Would require reporting cybersecurity incidents to Texas Homeland Security Division.)
  Referred to Border Security

Legislative Updates

HB 717
Public School Cybersecurity

- Would require TEA to create minimum cybersecurity controls to be implemented by LEAs.
- Would allow DIR to contract with LEAs to provide various cybersecurity services.
- Would allow Charter schools to utilize the Regional Security Operations Centers (RSOCs)

Texas Education Agency

Texas K12 Cybersecurity Program Preparation

April 2023

Purpose of Texas K12 Cybersecurity Program

- Immediate solutions to protect Local Education Agencies (LEAs) from major cyber incidents until LEAs can transition to the State funded Regional Security Operation Centers (RSOCs) and get full service.
- Priority will be given to rural LEAs
- Priority is to get Endpoint Detection and Response (EDR) onboarded and operational to as many LEAs as possible.
- Cybersecurity assessments will provide baseline of the cybersecurity maturity of LEAs.
- Network Detection and Response (NDR) for schools with cameras and other Internet of Things (IoT) devices.
- Cybersecurity practitioners will assist with implementation.

Preparation for Texas K12 Cybersecurity Program

In anticipation of the

TEA Cybersecurity Program

launch next fiscal year, we would like LEAs positioned to be able to receive security services as soon as possible.

Based on current planning:

- **Managed Security Service (MSS)** from Department of Information Resources (DIR)
- **Provide select security services**
- **Free of charge for LEAs**

DIR – Managed Security Services (MSS)

- **Risk and Compliance**
  - Cybersecurity Assessments
- **Security Monitoring and Device Management**
  - Endpoint Detection and Response
- **Incident Response**

(Services available via MSS will not be funded by Texas K12 Cybersecurity Program)

How Does K12 Cybersecurity Program Work?

LEA – Customers receiving services from MSS

ESC – Partners with TEA, DIR, and MSS Vendor to assist LEAs with implementing MSS services

TEA – Funds the K12 Cybersecurity Program and provide program standardization and facilitation

DIR – Texas State agency that provides IT services, including assessments, to Texas public sector organizations. All DIR contracts are competitively procured and comply with all state purchasing requirements.

MSS Vendor – The vendor contracted with DIR to provide security services to state and local government organizations; AT&T is the current MSS vendor.

MSI Vendor - The vendor contracted with DIR to provide the tools, processes, and invoicing to state and local government organizations; Capgemini is the current MSI vendor.

How Does K12 Cybersecurity Program Work?

1) Preparation

April – August 2023

LEAs that are interested in receiving cybersecurity services either independently or under the K12 Cybersecurity Program should begin to work with MSS vendor and DIR to complete the initial paperwork needed.

Fill out Customer Form and email to:
DIRSharedServices@dir.texas.gov

2) Choose your own adventure

Assessments:
MSS vendor conducts a virtual K12 modified Texas Cybersecurity Framework assessment.

Select Cybersecurity Technical Controls:
LEA/ESC requests solution via MSS portal. DIR provisions licenses for LEA. MSS vendor works with ESC or LEA to schedule and assist with implementation.

Technical Assistance for Cybersecurity Program Implementation: (MSS not required)
Contact your ESC for a list of implementation services available to your LEA and schedule the work.

3) Follow-up

Assessments:
MSS vendor delivers the report to the LEA and discusses remediation recommendations.

TEA reviews aggregate reporting to prioritize remediation support to LEAs in the future.

Select Cybersecurity Technical Controls:
TEA receives report from DIR on successful license implementation at LEA.

What is the Paperwork Involved?

Inter-Local Contract (DIR)

- Contract between DIR and LEA
- Contains general provisions pertaining to all services offered in DIR's Shared Technology Services (STS) program.

MSS Terms and Conditions (DIR)

- Terms and Conditions that pertain to the full-range of services offered within the MSS program.
- Written acceptance by the LEA to DIR

Solution Proposal Package (MSS Vendor)

- Similar to Scope of Work (SOW)
- Service Verification Meeting: Discusses work to be done in the assessment or implementation of security controls.
- Provision stating TEA is funding these services.
- TEA Certifications and Disclaimers

Inter-Local Contract

DIR Shared Technology Services
New Customer Form

- Please fill out the below information to establish your DIR Shared Technology Services account.
- E-mail completed form (with W-9 if you are not a state agency) to DIRSharedServices@dir.texas.gov
- Upon receipt of your information, a DIR representative will contact you to set up your Interagency/Interlocal Contract (IAC/ILC) and gather any additional required information.

You may tab from one field to the next.

General Information and Eligibility

The DIR Shared Technology Services Program is available to all state agencies and other governmental entities. If not a state agency, please attach W-9 with this form to confirm your eligibility.

Agency or Organization Name:	Agency/Entity Name
Agency or Organization Acronym	Agency/Entity Acronym
Comptroller or Federal Taxpayer ID Number (as shown on W-9):	##########
Type of Government Entity:	Entity Type (e.g., state agency, local government, etc.)
Six Digit Agency Code (if Applicable):	######

Customer Contacts

(If you have contacts with shared email accounts, we will only be able to assign that mailbox to one person.)

InterAgency Contract (IAC) Contact

The IAC contact will be responsible for reviewing and signing the IAC between your organization and DIR.

Name:	IAC Contact Name
Title:	Title
Address:	Street Address (Street/PO Box)
	City, TX Zip Code (City), (State) (Zip)
Telephone Number:	(###) ###-#### Ext:
E-mail:	first.last@agency.texas.gov

Inter-Local Contract

Service Operations Contact

The Service Operations Contact will be responsible for providing information to set up your services and will act as the day to day Customer Representative, including requesting/approving services through the online Portal, after services are established. This person will also receive all legal notices.

☐Same as Main Contact

Name:	Service Operations Contact Name
Title:	Title
Address:	Street Address (Street/PO Box)
	City, TX Zip Code (City) (State) (Zip)
Telephone Number:	(###) ### #### Ext:
E-mail:	first.last@agency.texas.gov

Inter-Local Contract

DIR Shared Technology Services
New Customer Form

Primary Finance Contact

The Primary Finance contact will be responsible for reviewing invoices, including accessing the online billing system, and ensuring payment is submitted timely.

☐Same as Main Contact

Name:	Primary Finance Contact Name
Title:	Title
Address:	Street Address (Street/PO Box)
	City, TX Zip Code (City), (State) (Zip)
Telephone Number:	(###) ###-#### Ext:
E-mail:	first.last@agency.texas.gov

Backup Finance Contact

The Backup Finance Contact serves as the backup to the primary finance contact, with the same access to review invoices and ensure payment is submitted timely.

Name:	Backup Finance Contact Name
Title:	Title
Address:	Street Address (Street/PO Box)
	City, TX Zip Code (City), (State) (Zip)
Telephone Number:	(###) ###-#### Ext:
E-mail:	first.last@agency.texas.gov

Inter-Local Contract

DIR Shared Services

Select the DIR Shared Services you are currently interested in:

- ☐ Email (Microsoft Office 365)
- ☐ Managed Services – Server and Storage
- ☐ Managed Services – Application Development/Maint
- ☒ Managed Services – Security
- ☐ Disaster Recovery as a Service (DRaaS)
- ☐ Backup as a Service (BUaaS)
- ☐ Print/Mail
- ☐ Texas.gov Services

Indicate any additional DCS services you may be interested in:

- ☐ Email (Microsoft Office 365)
- ☐ Managed Services – Server and Storage
- ☐ Managed Services – Mainframe
- ☐ Print/Mail
- ☐ Texas Imagery
- ☐ Backup as a Service (BUaaS)
- ☐ Disaster Recovery as a Service (DRaaS)
- ☐ Open Data Portal

Thank you for your interest in the Texas Shared Technology Services Program. Please email this form to DIRSharedServices@dir.texas.gov and we will contact you to set up your IAC/ILC, gather information about your environment, and discuss the steps to initiate service.

After filling out New Customer Information Form

- Review, sign, and accept Inter-Local Contract (ILC) with the Managed Security Services (MSS) Terms and Conditions. This document allows the LEA to procure services through DIR from our service providers. This will be sent to the contact on page 1 of the New Customer Information Form.
- Onboard the Service Contact on the New Customer Information Form to the STS Portal – this portal allows the ESC to make requests for services, review proposed services and review any associated costs with those services.
- Once DIR has received the signed ILC, LEA can put in a request for services in the STS Portal. (TEA funds after September 1st)

Additional Questions or Assistance?

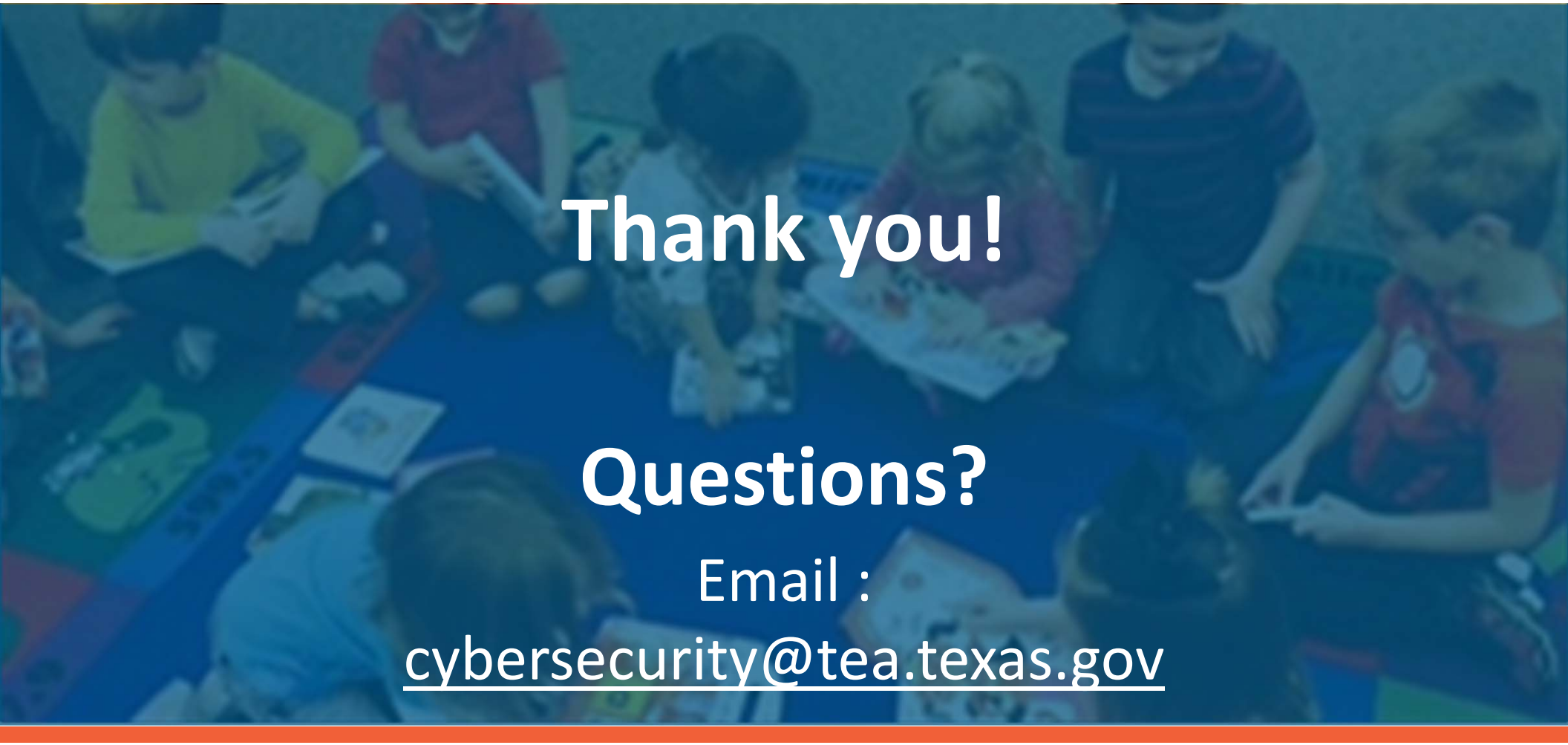
Contact cybersecurity@tea.texas.gov

OR

Contact the Texas Department of Information Resources CISO Office at DIRSecurity@dir.texas.gov

Texas Education Agency

Questions/Open Discussion



Thank you!

Questions?

Email :

cybersecurity@tea.texas.gov