Texas Education Agency

Cybersecurity Coordinator Forum

Todd Pauley, CISSP, CISM

Deputy CISO/Cybersecurity Coordinator

Texas Education Agency

todd.pauley@tea.texas.gov

February 28, 2024

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)
  - Information Security Forum (ISF) for Texas Government
  - State-Local Cybersecurity Grant Program (SLCGP) Update
  - Cybersecurity Advisory
  - Legislative Update
- Texas K12 Cybersecurity Initiative Update
- University of Texas at Austin: Strauss Center
  - Francesca Lockhart – Cybersecurity Clinic Program Lead

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.

Information Security Forum (ISF)

ISF 2024

Information Security Forum for Texas Government

25th ANNUAL INFORMATION SECURITY FORUM

Registration is now open for ISF!

April 2-3, 2024

Austin, TX

https://xcelevents.swoogo.com/isf2024attendee

The event is free for K-12 and public entities, but it will fill up fast.

State and Local Cybersecurity Grant Program (SLCGP)

CISA Cybersecurity Grant

Texas was allocated approximately $40 million over four years. The allocation requires matching funds that increase through the years. (Note: Matching funds will be paid by grant sub-recipients.)

- Texas' Cybersecurity Grant Charter was submitted and approved by CISA.
- The allocation is broken up into 4 years with awards happening individually in each year.
- A minimum of 80% of allocations must be passed through to local governments.
- At least 25% of the total funds made available under the grant must be passed through to rural communities.
- For FY22, Texas was allocated $8,469,945. The state matching fund requirement for FY22 is 10% and will be $846,994.50. So, there is a total of $9,316,939.50 available to be spent on cybersecurity projects for FY22.

https://dir.texas.gov/information-security/state-and-local-cybersecurity-grant-program-slcgp

State and Local Cybersecurity Grant Program (SLCGP)

CISA Cybersecurity Grant

- Eligibility Requirements:
  - Sign-up and participate in these free CISA services:
    - Web Application Scanning
    - Vulnerability Scanning
    - Nationwide Cybersecurity Review (NCSR)
  - Join the TX-ISAO (free).
  - Sub-recipients are also strongly encouraged to join the MS-ISAC.
  - ISD and Charter Schools are both eligible.

State and Local Cybersecurity Grant Program (SLCGP)

CISA Cybersecurity Grant

Priorities outlined in the Notice of Funding Opportunity (NOFO):

- Implement multi-factor authentication;
- Implement enhanced logging;
- Data encryption for data at rest and in transit;
- End use of unsupported/end of life software and hardware that are accessible from the Internet;
- Prohibit use of known/fixed/default passwords and credentials;
- Ensure the ability to reconstitute systems (backups); and
- Migration to the .gov internet domain.

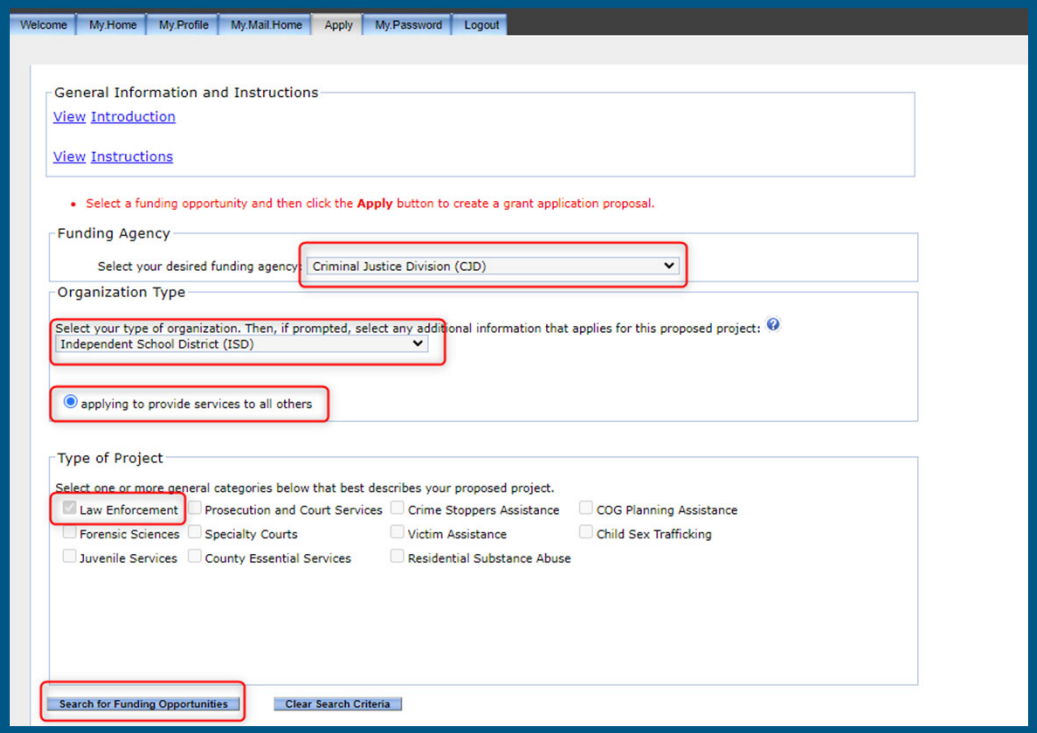
State and Local Cybersecurity Grant Program (SLCGP)

CISA Cybersecurity Grant

- Application Process:
  - The Office of the Governor (OOG) has published the request for applications (RFA) and will be open for submissions through March 14, 2024.
  - Eligible applicants will be able to apply through the OOG eGrants website:
    https://egrants.gov.texas.gov/Default.aspx
  - Funding for projects will be released within forty-five days after approval by the Department of Homeland Security's (DHS) Cybersecurity Infrastructure Security Agency (CISA).

State and Local Cybersecurity Grant Program (SLCGP)

CISA Cybersecurity Grant



Navigating the eGrants website:

1. Login to egrants.gov.texas.gov
2. Go to the Apply tab at the top
3. Select your desired funding agency "Criminal Justice Division (CJD)"
4. Type of organization is "Independent School District (ISD)"
5. Select "applying to provide services to all others"
6. Type of project is: "Law Enforcement"
7. Then "Search for Funding Opportunities" and it pulls up

Texas Education Agency

Cybersecurity Advisories

Multiple Vulnerabilities in FortiOS Could Allow for Remote Code Execution

Multiple vulnerabilities have been discovered in FortiOS, the most severe of which could allow for remote code execution. FortiOS is Fortinet's operating system used across many Fortinet devices. Successful exploitation of the most severe of these vulnerabilities could allow for remote code execution in the context of the system. Depending on the privileges associated with the service account, an attacker could then install programs; view, change, or delete data. Service accounts that are configured to have fewer user rights on the system could be less impacted than those who operate with administrative user rights.

THREAT INTELLIGENCE:

- Fortinet reports that CVE-2024-21762 is potentially being exploited in the wild.

SYSTEMS AFFECTED:

- FortiOS versions 6.0, 6.2, 6.4, 7.0, 7.2, 7.4, and 7.6. FortiProxy versions 7.0, 7.2, and 7.4.

https://www.cisecurity.org/advisory/multiple-vulnerabilities-in fortios-could allow-for-remote-code-execution_2024-019

Cybersecurity Advisories

LockBit Takedown and Beyond

"Operation Cronos" saw the takedown of 34 servers across Europe, the U.K. and the U.S.

Seizure of more than 200 cryptocurrency wallets, and the arrests of two alleged LockBit members in Poland and Ukraine.

LockBit claims to have restored from backups and are unaffected by the government takedown.

LockBit's administrator said after "5 years of swimming in money I became very lazy" and overlooked a PHP vulnerability. They also threatened to retaliate by saying it would target the government sector.

Also, they are threatening to release files they claim to have from Fulton County, Georgia regarding certain high profile court cases there by March 2nd unless a ransom is paid.

The government says LockBit has claimed more than 2,000 victims worldwide and extorted over $120 million in payments.

Sources: https://techcrunch.com/2024/02/26/lockbit-ransomware-takedown-now-what/
https://www.scmagazine.com/news/lockbit-returns-after-takedown-with-new-extortion-threats

Cybersecurity Advisories

SVR Cyber Actors Adapt Tactics for Initial Cloud Access

Russian Foreign Intelligence Service (SVR) cyber actors have targeted governmental, think tank, healthcare, and energy targets for intelligence gain. It has now observed SVR actors expanding their targeting to include aviation, education, law enforcement, local and state councils, government financial departments, and military organizations.

Mentioned techniques:

- Access VIA service and dormant accounts
- Cloud-Based token authentication
- Enrolling new devices to the cloud
- Residential Proxies

https://www.cisa.gov/news-events/cybersecurity advisories/aa24-057a

Local Government Incident Reporting (SB 271)

New Reporting Process

- Incidents will be submitted using Archer Engage
- After creating an account, users can submit incidents and then the closure/post-mortem form
- This will replace the current School District Incident Report, required by Section 11.175 of the Education Code

https://dir.texas.gov/information-security/cybersecurity-incident-management-and-reporting/sb-271-security-incident

Legislative Update

HB 18 (SCOPE)

TEA released a TAA late last year that included ‘Standards for Electronic Devices and Software Applications’

https://tea.texas.gov/about-tea/news-and-multimedia/correspondence/taa-letters/standards-for-permissible-electronic-devices-and-software-applications

HB 18 Protection of minors on digital services and devices:

- Requires users to register with their age for a digital services and social media.
- Minors will need parental consent.
- Reduce marketing content to minors
- TEA shall adopt standards for permissible electronic devices and software used by a school district.
- When issuing a device, LEAs must “install an Internet filter that blocks and prohibits pornographic or obscene materials or applications, including from unsolicited pop-ups, installations, and downloads.”
- Establishes a joint committee of the legislature to study the effects of media on minors.

Texas Education Agency

Texas K12 Cybersecurity Initiative

February 2024

Texas K12 Cybersecurity Program Outreach

- Eligibility for fully funded Endpoint Detection and Response (EDR) includes LEAs with student enrollment of 15,000 or less. Initial distribution should prioritize servers and staff, with a maximum limit of licenses equal **20%** of student enrollment.
- 30 EDR license minimum for smaller districts.
- As of 2/23/23:
  - 95,307 EDR clients approved.
  - 32,733 EDR clients installed and active.
- Other cybersecurity services are on a first come first serve basis and will include Cybersecurity Assessments and Network Detection and Response (NDR).
- Cybersecurity Assessments – TEA and DIR have agreed on the process and scope of the assessments. DIR is waiting for an official approval internally.
  - **Details on Assessments should be able available in the March CCF Webinar.**

Texas K12 Cybersecurity Program Outreach

The following cybersecurity controls are highly encouraged for all LEAs to implement and fall within the scope of this initiative:

- Implement fully managed Endpoint Detection and Response (EDR) on LEA servers and applicable staff devices. TEA will fully fund licenses with limited distribution. See details below.
- Implement Multi-Factor Authentication (MFA) on staff email systems.
- Implement email protocol security configurations.
- Restrict local admin access.

Resources, Questions or Assistance?

Contact cybersecurity@tea.texas.gov

OR

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

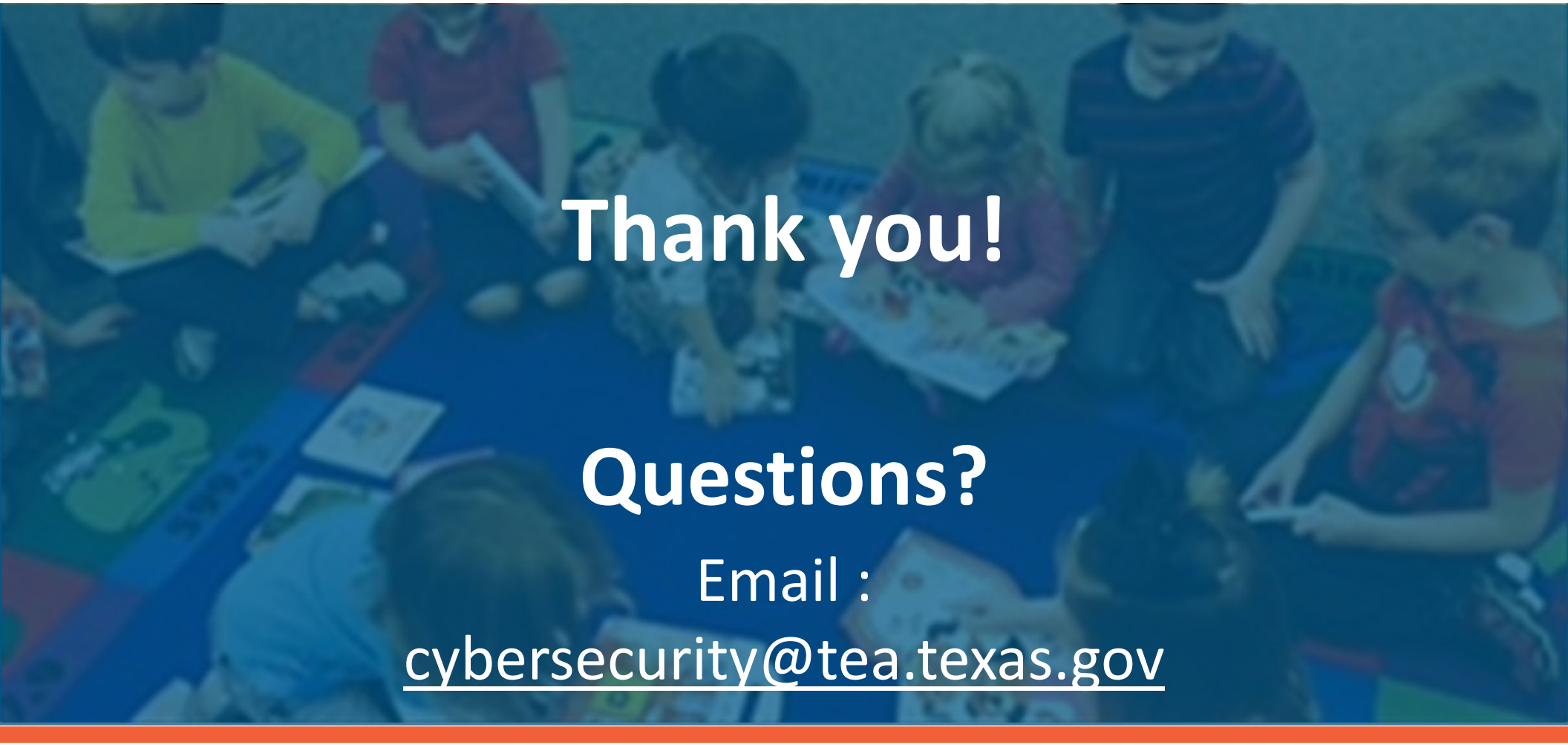
TEA K-12 Cybersecurity Initiative Webpage

https://tea.texas.gov/academics/learning-support-and-programs/technology-planning/k-12-cybersecurity-initiative

Texas Education Agency

Strauss Center – UT Austin

February 2024



Thank you!

Questions?

Email :
cybersecurity@tea.texas.gov