# Cybersecurity Coordinator Forum

February 2026

Daniel Ramirez

Chief Information Security Officer

Texas Education Agency

cybersecurity@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.

# House Keeping

- 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.

# About Me

## 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)

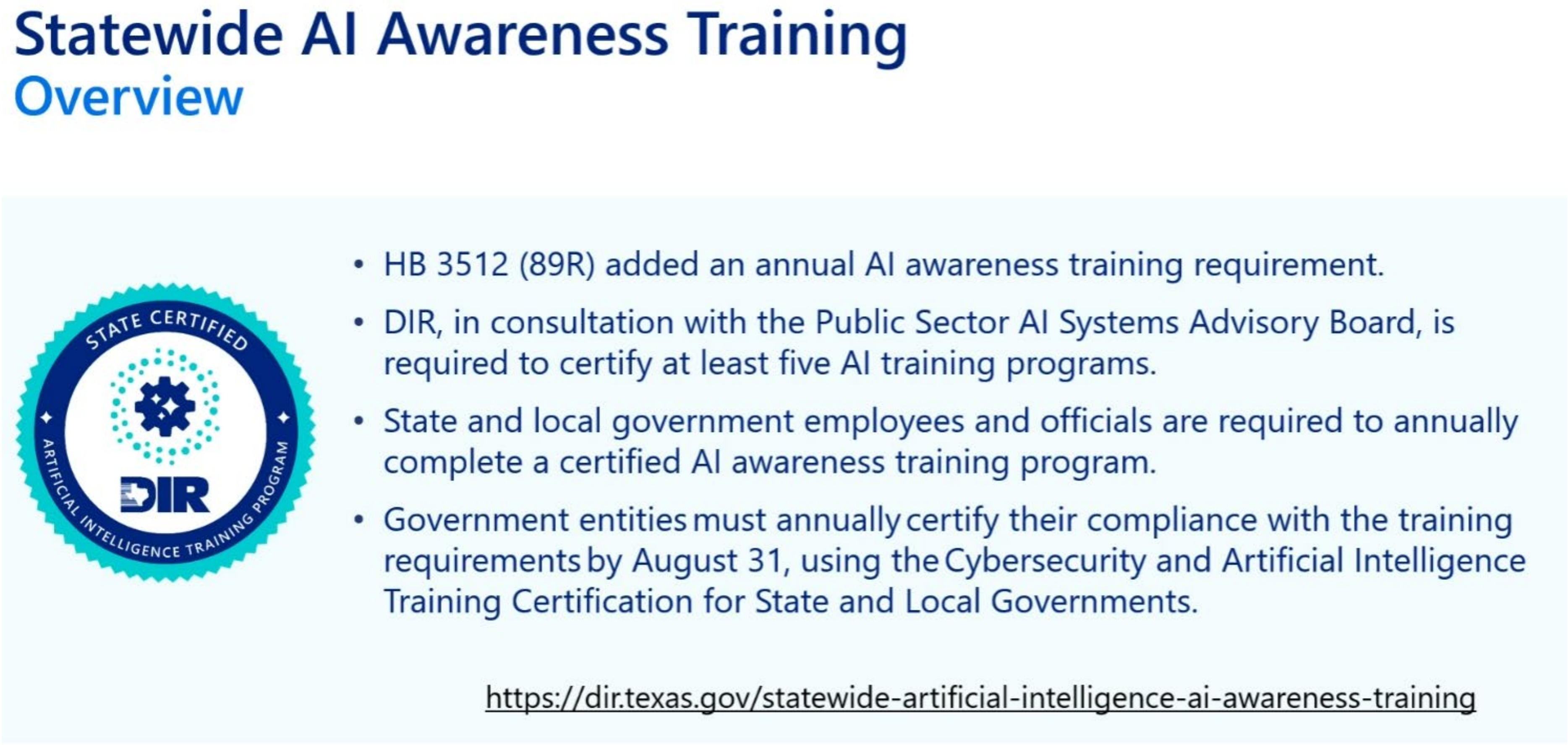
Texas Education Agency

# Security Awareness Training

# 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

# Artificial Intelligence (AI) Training



## Statewide AI Awareness Training
### Overview

- HB 3512 (89R) added an annual AI awareness training requirement.
- DIR, in consultation with the Public Sector AI Systems Advisory Board, is required to certify at least five AI training programs.
- State and local government employees and officials are required to annually complete a certified AI awareness training program.
- Government entities must annually certify their compliance with the training requirements by August 31, using the Cybersecurity and Artificial Intelligence Training Certification for State and Local Governments.

https://dir.texas.gov/statewide-artificial-intelligence-ai-awareness-training

# AI Awareness Training Requirements

- School Systems
  - Only cybersecurity coordinator required to complete annual AI training
  - 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

Texas Education Agency

# Federal Grant Compliance

# Federal Office of Management and Budget (OMB)

- 2 CFR § 200.303(e)
  - Requires federal award recipients and subrecipients to implement reasonable, risk-based cybersecurity and other safeguards to protect PII and sensitive information in compliance with applicable privacy and confidentiality laws.
  - Auditable under the Single Audit Act
  - Core internal control requirement tied directly to grant compliance
  - Review by TEA Grant Compliance and Administration

# Compliance

- Demonstrate reasonable, documented, and operational cybersecurity measures
  - Officially assigned Cybersecurity Coordinator {§11.175(d)}
  - Adopted a cybersecurity framework (e.g. Texas Cybersecurity Framework TCF) {§11.175(b)}
  - Annual cybersecurity awareness training compliance {§2054.5191}
  - Protection of devices and data
    - 24/7 Managed Endpoint Protection and Response
  - Incident Response Plan
    - Multihazard Emergency Operations Plan (EOP) Cybersecurity Annex

Texas Education Agency

# Texas K-12 Cybersecurity Initiative

# TEA K-12 Cybersecurity Initiative

- In response to the increasing threat of ransomware and other malicious cyber activity targeting school systems across Texas, the Texas Education Agency (TEA) launched the K-12 Cybersecurity Initiative in 2023. The initiative was made possible through funding approved by the 88th Texas Legislature, which supported 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 rural school systems, and cybersecurity practitioners are available through regional education service centers to support the implementation of cybersecurity controls aligned with the scope of this initiative.

# Ongoing Goals – K-12 Cybersecurity Initiative

- Current goals were 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 **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**).
    - Pilot is closed to new customers while pilot benefits & costs are evaluated.
- TEA funded grant thru Technology Alliance for Statewide Initiatives (TASI) that pays for cybersecurity staff at every Education Service Center (ESC) to assist with these goals.

**Domain-based Message Authentication Reporting & Conformance (DMARC)*

# Enrolling and Requesting Services

1. School system completes **New Customer Form,** sends 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 **Shared Technology Services (STS) Portal Access** is granted (to listed technical contacts on New Customer Form).
6. School system requests Managed Security Services (MSS) via STS Portal.
   1. EDR
   2. TCF Assessment

# Education Service Center (ESC) Support

- ILC & STS Onboarding Assistance
- EDR Agent Deployment
- Email Domain Security (SPF, DKIM, DMARC Compliance)
  - 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

*Sender Policy Framework (SPF)*
*Domain Keys Identified Mail (DKIM)*
*Domain-based  Message Authentication Reporting & Conformance (DMARC)*

# Current Program Participation

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

- **End Point Detection Response (EDR)**
  - 392 school systems have signed up for EDR.
  - Installed on 273,000 endpoints.
  - **48,000+** attacks blocked.
  - **17,000+** ransomware threats neutralized.

- **Texas Cybersecurity Framework (TCF) Assessments**
  - 71 LEAs have signed up; 47 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.

Texas Education Agency

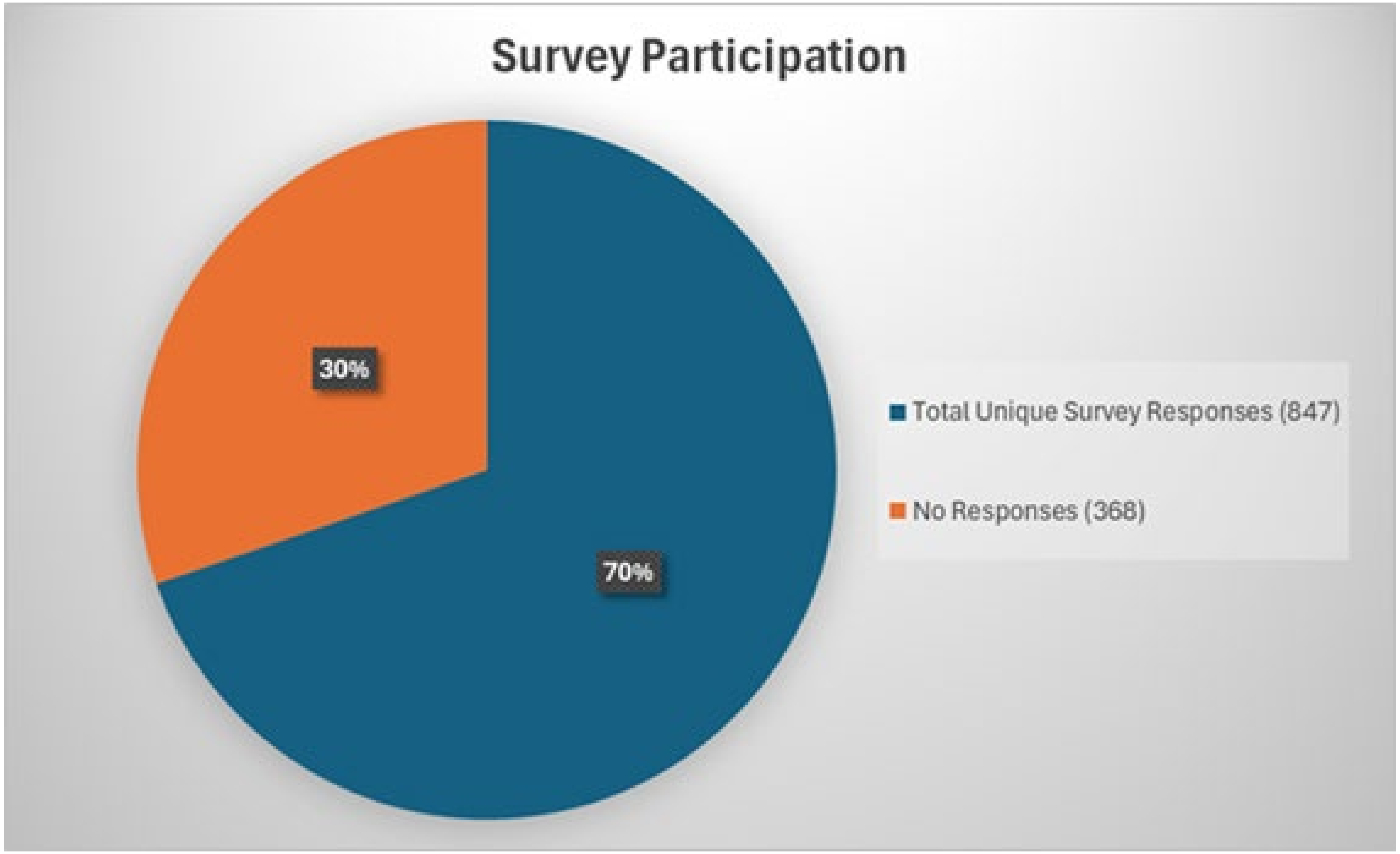
# K-12 Cybersecurity Initiative Survey

# K-12 Cybersecurity Initiative Survey

- September 29, 2025 – October 10, 2025
- The survey was intended to assess the impact of the K-12 Cybersecurity Initiative from Sept 2023 – Aug 2025, identify roadblocks to participation, and gather input on what cybersecurity services and supports would be most helpful in FY26/FY27 (Sept 2025 – Aug 2027).

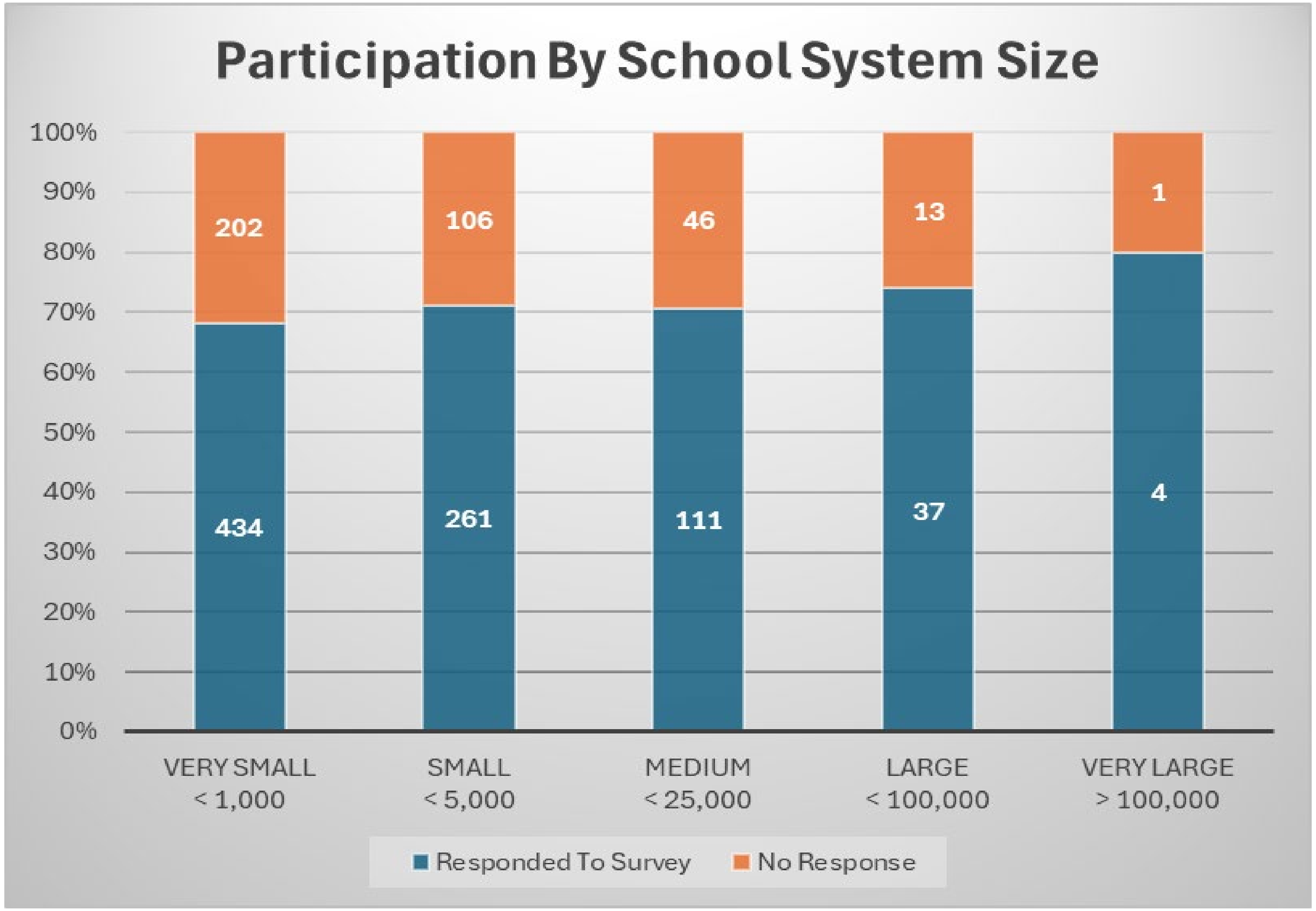
# K-12 Cybersecurity Initiative Survey Cont.

## 70% Survey Participation



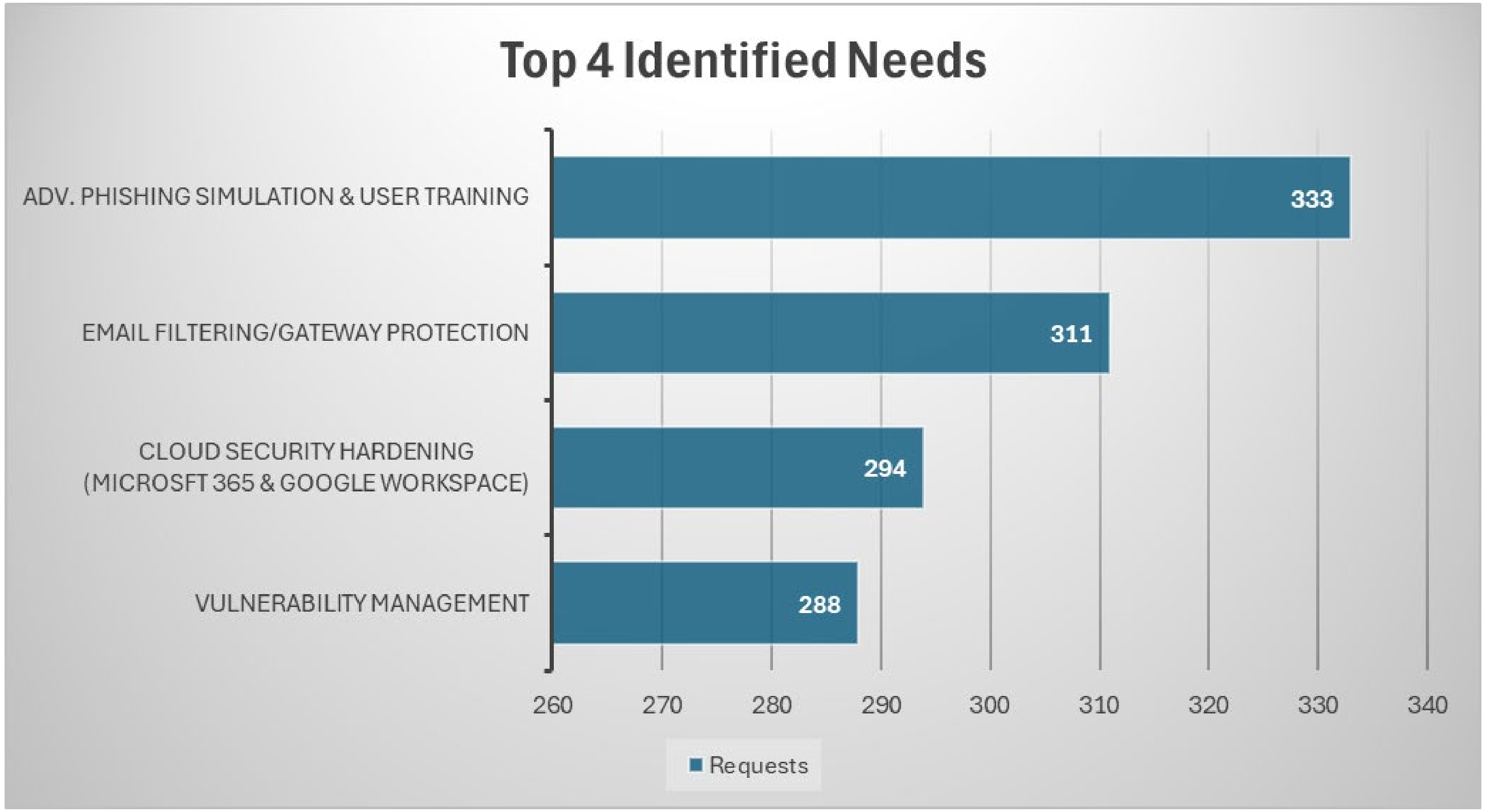
# K-12 Cybersecurity Initiative Survey…

## 70% Survey Participation



# K-12 Cybersecurity Initiative Expansion

- Survey Question: What Cybersecurity issues or services should be prioritized in the next phase of the initiative?



Texas Education Agency

# K-12 Cybersecurity Initiative Updates

# New Goals – K-12 Cybersecurity Initiative

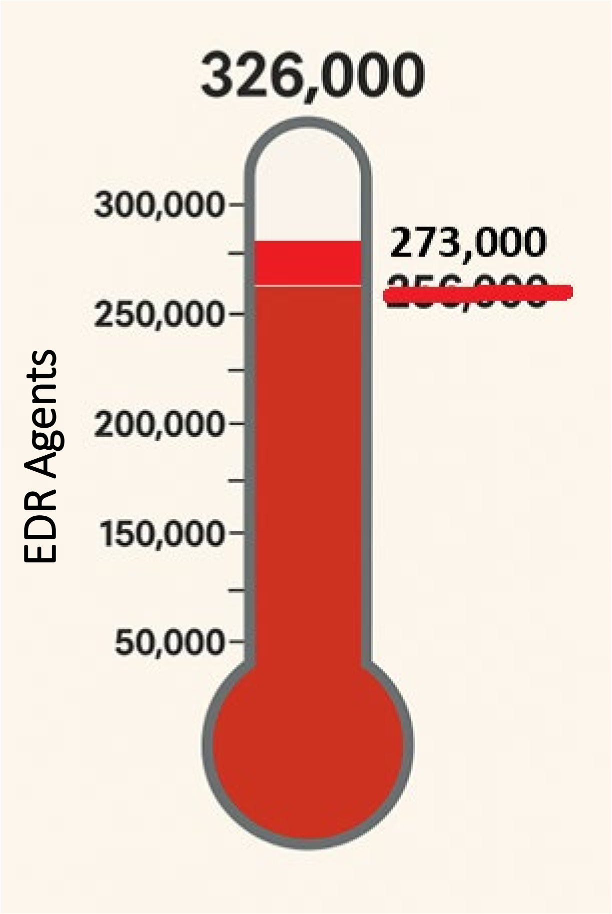
- **Cloud Email Security** – Provided in collaboration with the University of Texas (UT) Regional Security Operations Center (RSOC).

- DIR Certified **Security Awareness Training** and **Phishing Simulations** – Provided in collaboration with the Technology Alliance for Statewide Initiatives (TASI).

- **Microsoft365 & Google Workspace Hardening Guides** – Under development by TASI.

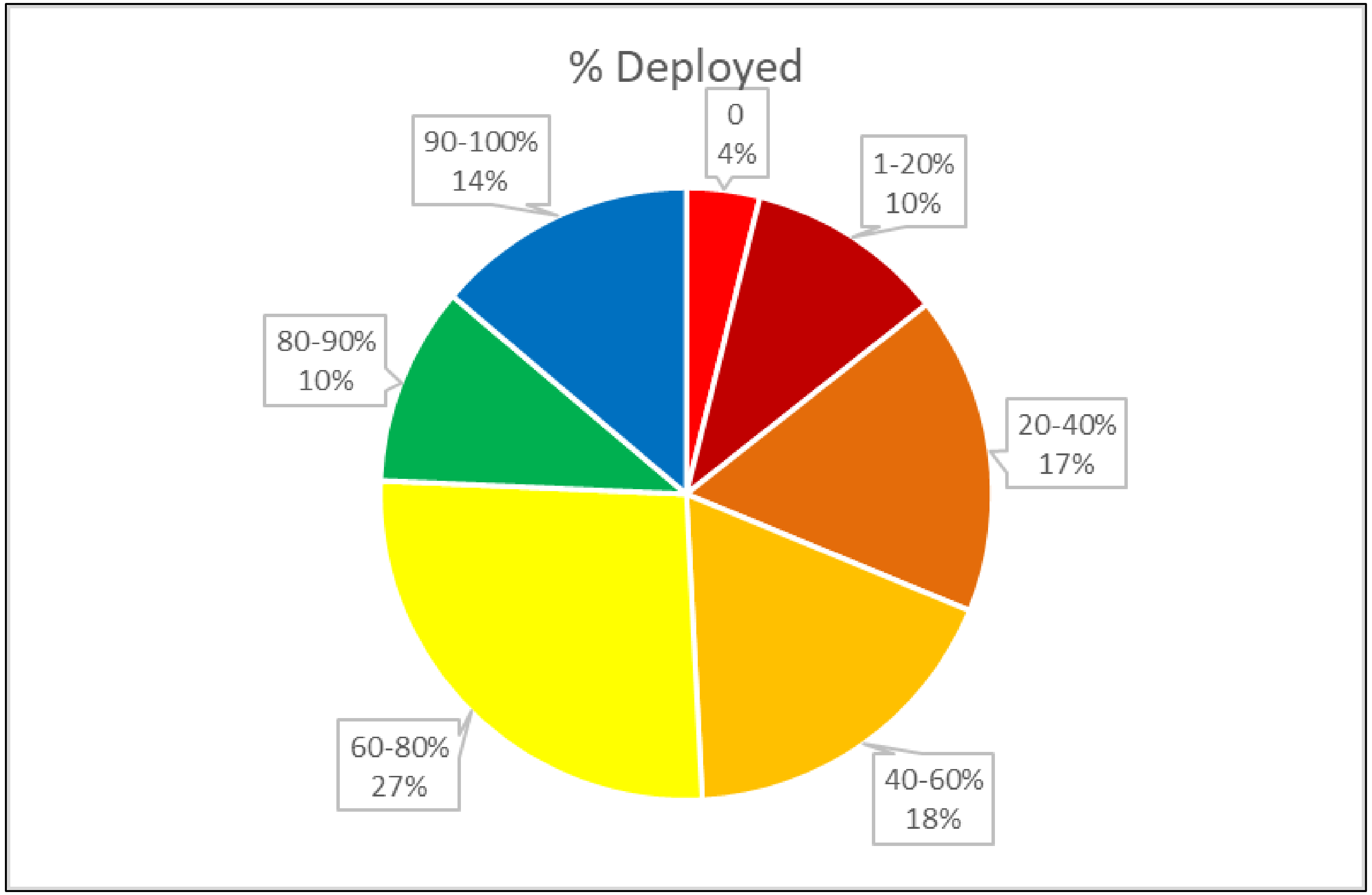
- **Software Deployment Solution** for rollout of EDR agents and other software – Provided in collaboration with TASI.

# EDR – First Come, First Served



- $35,000,000 for EDR
  - 65% of K-12 Cyber Initiative Budget
- 326,000 EDR Agents
- ~~256,000 Agents Deployed~~
  - ~~79% of 326,000~~
- 273,000 Agents Deployed
  - 84% of 326,000
- 433,000 Agents Approved
  - 133% of 326,000

# Current EDR Approved vs Deployed



| % Deployed | Count |
|---|---|
| 0 | 14 |
| 1-20% | 38 |
| 20-40% | 61 |
| 40-60% | 65 |
| 60-80% | 96 |
| 80-90% | 38 |
| 90-100% | 50 |
| **Total** | **362** |

# Approval Re-Alignment (for already approved requests)

- Approved EDR Requests prior to January 1, 2026
  - 60 Days starting February 1, 2026, to complete deployment.
  - On April 3rd, approved count is adjusted to current deployment + 10%.
  - **Example:**
    - ACME ISD is approved for 1,000 agents on June 1, 2025
    - 350 (35%) agents are deployed as of January 20, 2026
    - ACME deployment count reaches 450 on April 2, 2026
    - New approved count is adjusted to 495 (450 + 10%)
    - ACME ISD is 90% Deployed as of April 3, 2026
  - ACME ISD may submit an Add-On request if it determines additional agents are needed later. Approved only if additional agents are still available.
  - Maximum allowed will remain 30% of student enrollment, with a minimum of 30 agents and maximum of 15,000 agents.

# Approval Re-Alignment (new EDR requests)

- New EDR Requests (starting February 1st)
  - 90 Days to complete deployment.
  - After 90 days, approved count is adjusted to current deployment + 10%.
  - **Example:**
    - ACME ISD is approved for 1,000 agents on February 1, 2025
    - 350 (35%) agents are deployed as of May 2, 2026
    - New approved count is adjusted to 385 (350 + 10%)
    - ACME ISD is 90% Deployed on May 3, 2026
  - ACME ISD may submit an Add-On request if it determines additional agents are needed later. Approved only if additional agents are still available.
  - Maximum allowed will remain 30% of student enrollment, with a minimum of 30 agents and maximum of 15,000 agents.

# Re-Alignment Will:

- Encourage school systems to deploy to 100% of in-scope devices now.
- Forecast actual need and determine if/when additional funds will be needed.
- Allow TEA to determine if EDR may be opened to all school systems, including those above the 50,000 student enrollment max.
- Use up all funds allocated to EDR, currently $35,000,000.
- Once all 326,000 agents are approved and deployed, no more school systems will be approved for EDR service until additional funding is secured.

# K-12 Cyber Initiative EDR for In-scope Computers

- School systems need comprehensive EDR coverage
  1. On-premise 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 the list.

# New Cloud Email Security Service

- School system will be required to be DMARC compliant prior to or within 30 days of deployment.
- UT-RSOC will assist with deployment configuration, monitoring, and regular tuning as needed.
- UT-RSOC will provide TEA with aggregate reports on threats blocked and share common threats with state threat feeds.

# School System Cyber Support Options

- State provides funds in support of:
  - TEA funded cybersecurity services
    - Managed EDR
    - TCF Assessments
    - Cloud Email Security
    - Security Awareness Training & Phishing Simulations
    - NDR
    - School system support and training provided by ESCs
  - RSOC services
    - Incident Response Assistance
    - 24/7 Monitoring
      - Managed EDR
      - Cloud Email Security
    - Tabletop exercises
    - Threat Intelligence Sharing

**This list is not all inclusive.*

Texas Education Agency

# Wrapping Up

# Reminder – 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 all the above when Technology or Cybersecurity Coordinators change

# 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 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: March 25, 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