TEA®
Texas Education Agency

Texas K-12 Cybersecurity Initiative Update

March 2024

Cybersecurity Coordinator Forum

The **TEA Cybersecurity** team hosts a **monthly** meeting for Texas Local Education Agency (LEA) **Cybersecurity Coordinators,** Education Service Center (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:

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

Purpose of Texas K-12 Cybersecurity Initiative

- Establish and mature cybersecurity support for ESCs and LEAs long-term.
- Assist LEAs in prioritizing the most impactful preventions to major cyber events.

Fully Funded Services

- **Fully funded services currently available for request :**
  - To start request please *register*: New customer form
  - **Managed Endpoint Detection and Response (EDR)**
    - Requirement: student enrollment 15,000 or less, licenses up to 20% enrollment, 30 license min.
    - Once registered, request service via Managed Security Service (MSS): MSS Portal Log In Process (texas.gov).
    - LEAs may choose between EDR vendors Crowdstrike or SentinelOne.
    - Standard option should be most common for LEAs.
  - **School District Cybersecurity Assessment**
    - Requirement: First come, first served for any LEA.
    - Once registered, request service via MSS : TX K-12 Cybersecurity Assessment Quick Start Guide
    - LEAs may choose between Basic, Intermediate, or Advanced Cybersecurity Assessments.

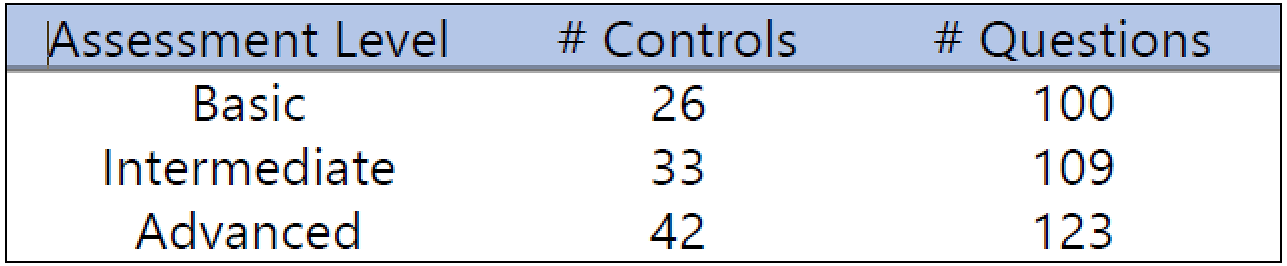
K-12 Cybersecurity Initiative | Texas Education Agency

School District Cybersecurity Assessment

- LEAs need an independent cybersecurity assessment completed to understand the effectiveness of their cybersecurity policy that was established in Texas Education Code 11.175.
- The School District Cybersecurity Assessment is an independent maturity assessment, based on the Texas Cybersecurity Framework (TCF). This assessment offering provides multiple tiers to choose from (Basic, Intermediate, and Advanced), which cover an increasing scope of controls from the minimum controls necessary for LEAs to the full scope of a standard TCF Assessment.
- Recommended remediation plans from the cybersecurity assessment will provide prioritized solutions to reduce risk where it is most needed in the K-12 environment.

School District Cybersecurity Assessment

- This service focuses on the maturity of processes, gaps against standards of good practice and compliance requirements, and risks to the organization, based on the TCF.
- The assessment will include interviews of key stakeholders and review of documentation.
- Output of the assessment is a formal report provided to the LEA with a security maturity designation level ranging from 0-5.
  - Note: Security maturity designation level of 2 is currently the average for educational institutions. The goal of K-12 Cybersecurity Initiative is to assist LEAs and ESCs to achieve a maturity designation level of 3, which reflects that LEAs have a documented framework in place that addresses all the control areas.



Assessment Level	# Controls	# Questions
Basic	26	100
Intermediate	33	109
Advanced	42	123

Upcoming Funded Services

- Upcoming Services via your Education Service Center:
  - Technical assistance to implement the following critical controls
    - **EDR**
    - **Multifactor Authentication** for staff email
    - **Email security protocol** (SPF, DKIM, and DMARC)
    - **Restrict local admin access**
- Upcoming Services
  - Network Detection and Response (NDR)

K-12 Cybersecurity Initiative | Texas Education Agency

TX K-12 Cybersecurity Initiative Participants

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 Initiative and provides program standardization and facilitation

DIR (Department of Information Resources) – 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 K-12 Cybersecurity Initiative Work?

1) Preparation

Now

LEAs that are interested in receiving cybersecurity services via DIR's Managed Security Service, either independently or under the K-12 Cybersecurity Initiative should begin to work with ESC and MSS vendor to complete the initial paperwork needed.

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

2) Choose your own adventure

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.

Assessments:
MSS vendor conducts a virtual K-12 modified Texas Cybersecurity Framework assessment.

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

3) Follow-up

Select Cybersecurity Technical Controls:
TEA receives report from DIR on successful license implementation at LEA as well as threat blocking activity.

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.

What is the Paperwork Involved?

Register:

[New customer form]

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.

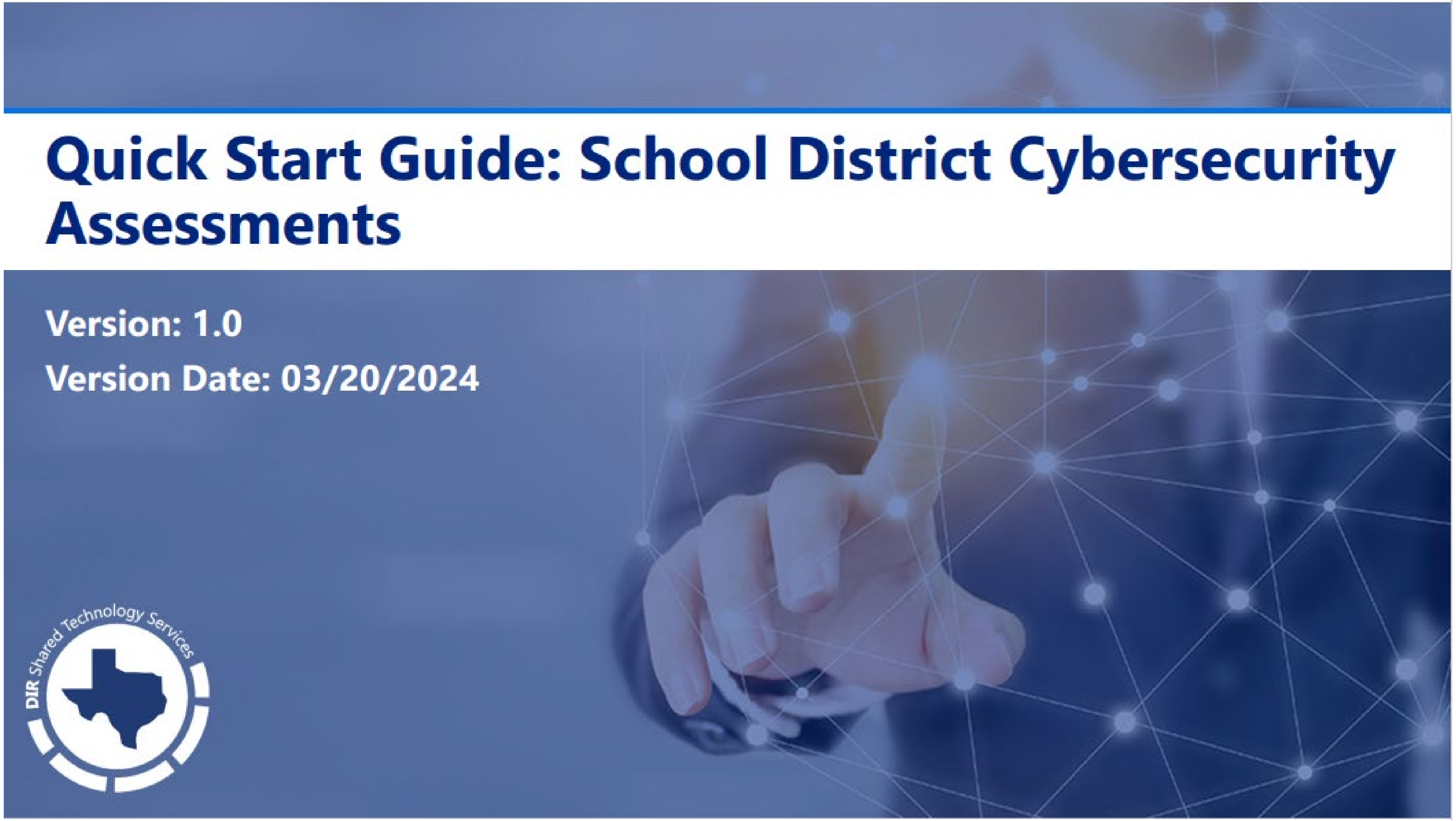
MSS Terms and Conditions (DIR)

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

Technical Provisioning Document (TPD) (MSS Vendor)

- 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

Quick Start Guide: School District Cybersecurity Assessments



Quick Start Guide: School District Cybersecurity Assessments

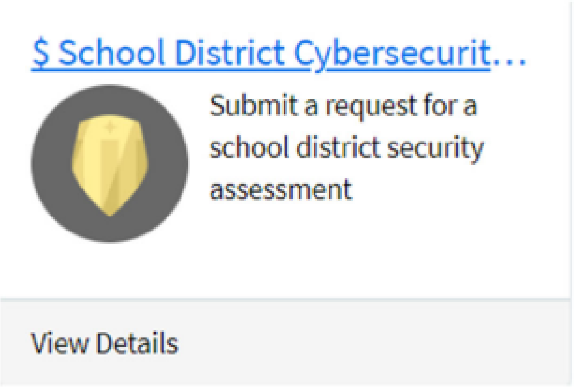
Version: 1.0

Version Date: 03/20/2024

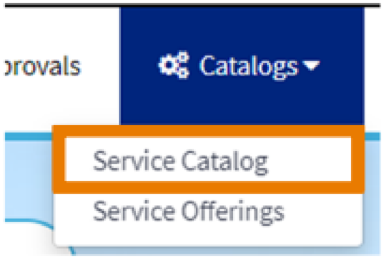
Quick Start Guide: School District Cybersecurity Assessments

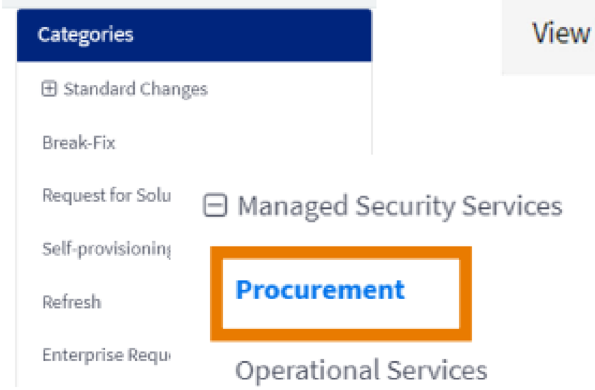
Requesting School District Cybersecurity Assessments

1. From the STS portal hover over catalogs at the top and select service catalog from the drop down.
2. Expand the Managed Security Services option from the Categories panel and click on Procurement.
3. Click on $ School District Cybersecurity Assessment.


$ School District Cybersecurit…

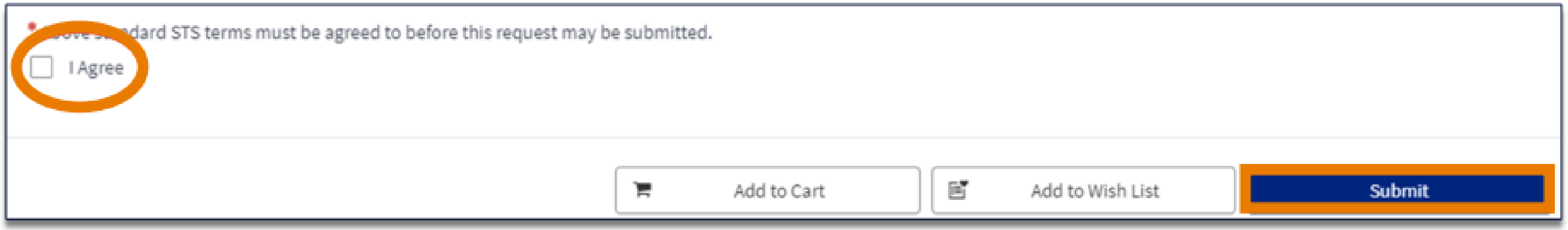
Submit a request for a school district security assessment





Requesting School District Cybersecurity Assessment– Cont.

1. Complete all required fields marked with an asterisk.
2. Check the "I Agree" to the terms box and click Submit.



* Above standard STS terms must be agreed to before this request may be submitted.

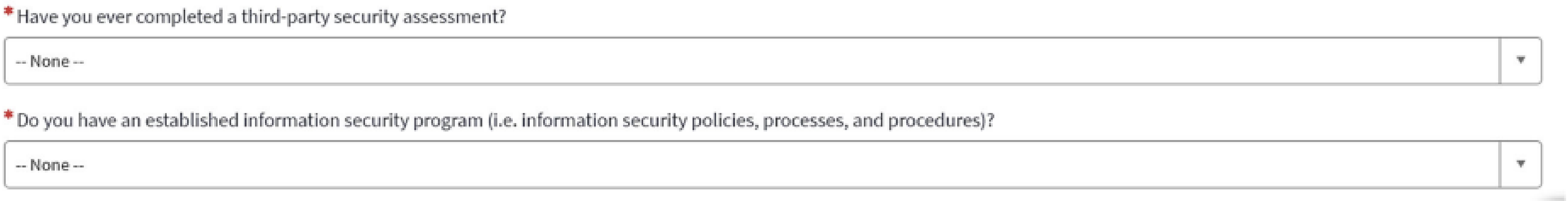
□ I Agree

Next Steps

1. The request is routed for TEA funding approval.
2. MSS (AT&T) will contact you to verify the request and schedule a start date.

School District Cybersecurity Assessment Additional Information

- The questions below are to help MSS better understand your environment. If you are not sure of the answer, please select unknown from the dropdown.



*Have you ever completed a third-party security assessment?

-- None --

*Do you have an established information security program (i.e. information security policies, processes, and procedures)?

-- None --

Additional Questions or Assistance?

ESC Contact:

TASIK12Cybersec@tasitx.org

K-12 Cybersecurity Initiative | Texas Education Agency