Texas Education Agency

To the Administrator Addressed

Commissioner Mike Morath

1701 North Congress Avenue • Austin, Texas 78701-1494 • 512 463-9734 • 512 463-9838 FAX • tea.texas.gov

DATE:	**June 15, 2023**
SUBJECT:	**TX K-12 Cybersecurity Initiative**
CATEGORY:	**Cybersecurity Funding Opportunity for LEAs**
NEXT STEPS:	**Share with district administration and technology staff**

To counter the rising surge of ransomware and malicious activity affecting local education agencies (LEAs) around the state, the Texas Education Agency (TEA) submitted an exceptional item request for funding to the Texas Legislature to provide cybersecurity resources to LEAs. We are pleased to announce that our request has been approved, and we will be able to distribute these **funds for certain purchases made between September 1, 2023 and August 31, 2025.**

From the legislative entry into the budget:

> *It is the intent of the Legislature that the Texas Education Agency enter into an interagency agreement with the Department of Information Resources (DIR) to provide cybersecurity services for LEAs in accordance with DIR Strategy C.1.2, Security Services. Cybersecurity services to be provided by DIR may include, but are not limited to, cybersecurity assessments, end point detection response, and network detection response.*

PURPOSE AND SCOPE OF INITIATIVE

The purpose of this initiative is to provide immediate solutions to protect LEAs from major cyber incidents, such as ransomware. Priority will be given to rural LEAs, and cybersecurity practitioners will be available at your regional education service center to assist with implementation of cybersecurity controls that fall within scope of this initiative.

The following cybersecurity controls are highly encouraged for all LEAs to implement between September 1, 2023 and August 31, 2025 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. More details to come.
- Implement email protocol security configurations. More details to come.
- Restrict local admin access. More details to come.

The following cybersecurity controls are funded on a first come first served basis by TEA through DIR's Shared Technology Services (STS) program and are recommended to mature LEA cybersecurity posture. These controls fall within scope of this initiative:

- Complete a third party K-12 Cybersecurity Assessment to get a baseline of your cybersecurity maturity and action plan for improving cybersecurity posture. Application to open in September.
- Implement Network Detection and Response (NDR), especially for schools with cameras and other Internet of Things (IoT) devices. Application to open in September.

INTER-LOCAL AGREEMENT WITH DIR SHARED TECHNOLOGY SYSTEM REQUIRED

LEAs will need to sign DIR's inter-local agreement to receive the in scope services from DIR's Shared Technology Services (STS), Managed Security Services (MSS) program. Our goal is to have all eligible LEAs onboarded with a signed inter-local agreement by

September 1, 2023, so the services can be distributed as soon as possible. After the inter-local agreement is in place, eligible LEAs may then request in scope services through the STS program, which will be paid for by TEA starting September 1, 2023 through August 31, 2025. The MSS vendor, AT&T, or your regional education service center may reach out to your LEA to help facilitate this process. Details about this process were discussed in the April Cybersecurity Coordinator call, and a recording can be accessed here, which includes additional resources with instructions and scope: https://tea.texas.gov/academics/learning-support-and-programs/technology-planning/k-12-cybersecurity-initiative

You may register for the Cybersecurity Coordinator Forum series at this URL using your LEA email address: https://attendee.gotowebinar.com/register/8234183618339320587
The next scheduled webinar is scheduled for June 28th @ 11am CDT.

LIMITED DISTRIBUTION OF EDR PER LEA ENROLLMENT

It is TEA's intention to focus on small and rural LEAs for the distribution of Endpoint Detection and Response (EDR) services through DIR's Managed Security Services (MSS). The EDR provided, which replaces traditional anti-virus software and incorporates threat intelligence along with malicious behavior characteristics on endpoints, will be fully managed to eliminate additional LEA overhead and is one of the best solutions to prevent ransomware and secure devices. The current vendors under the MSS contract for EDR are CrowdStrike and SentinelOne. To provide a scope that we can reasonably accommodate with the funding provided, **TEA will limit the distribution for LEAs with a total enrollment of 15,000 and below, with a range from 30 licenses up to licenses equal to 10% of student enrollment, whichever is larger.** It is TEA's intent to **focus on high-risk and impact devices,** so **initial distribution should focus on servers and central office staff with any remaining licenses distributed to other staff devices that have access to sensitive data.** .

SECURITY ASSESSMENTS BASED ON SAMPLING OF LEAs BY SIZE

Security assessments will also be available to LEAs as part of this initiative and will also be provided by AT&T through DIR's services catalog. The intent of these assessments is to provide a high-level look at the overall state of cybersecurity in Texas' K-12 public entities. TEA will not receive detailed copies of reports for any individual LEA. **Scope of and availability of the assessments will be based on a sampling of LEAs by size.** Once those assessments are set up in the STS program, we will provide guidance to interested parties on how to request those assessments through the STS program.

DORKBOT SERVICE

Finally all LEAs will be signed up with the Dorkbot web application vulnerability notification service. Dorkbot is an automated system run by the University of Texas – Austin, that uses publicly available information to identify vulnerable public facing systems on K-12 networks. Currently designated cybersecurity coordinators for each LEA will be the point of contact for any findings the service uncovers, so please ensure those designations are up to date in AskTED. Please reach out to your district AskTED coordinator or email askted@tea.texas.gov if you need assistance with updating AskTED.

The Dorkbot service for LEAs will begin July 1, 2023.

More information about the Dorkbot service can be found at:
https://security.utexas.edu/dorkbot

Any LEA wishing to opt-out of the free service, can do so by emailing cybersecurity@tea.texas.gov.