KCSD

Kenton County School District | *It's about ALL kids.*

Issue Paper

DATE:
04/23/2024

AGENDA ITEM (ACTION ITEM):
Consider/Approve utilizing services provided by Cybersecurity and Infrastructure Security Agency (CISA) under the Department of Homeland Security (DHS) to assist Kenton County Technology Department in providing higher levels of Cyber Security, enhanced procedures, recommended security measures, and technology health checks.

APPLICABLE BOARD POLICY:
01.1 Legal Status of the Board

HISTORY/BACKGROUND:
KCSD Technology currently adheres to all policies and procedures related to Cybersecurity. With the ongoing and increased immediate cybersecurity threats, CISA has been able to create a portfolio of services to assist K12 districts across the United States in increasing our awareness beyond the baseline policies and procedures. These services allow for an internal and external deep dive into the systems, networks, and operations utilized by Staff and Students related to Technology. KCSD Technology have completed some initial scans and initial conversations on what CISA can offer and those services will drive deeper conversations and ultimately assist in revising policies, procedures, and practices to enhance the overall KCSD Technology Cybersecurity approach. The resources are free to KCSD and funded to CISA through the DHS network of government entities. Kentucky has a dedicated Cybersecurity Coordinator provided by CISA and we have already had multiple meetings that have led to the request to utilize more of these services to enhance the cybersecurity at KCSD.

FISCAL/BUDGETARY IMPACT:
No Budget Impact

RECOMMENDATION:
Approval to utilizing services provided by Cybersecurity and Infrastructure Security Agency (CISA) under the Department of Homeland Security (DHS) to assist Kenton County Technology Department in providing higher levels of Cyber Security, enhanced procedures, recommended security measures, and technology health checks.

CONTACT PERSON:
Matthew Winkler, Director of Technology

Matthew Winkler
Principal/Administrator

District Administrator

Superintendent

CYBER ASSESSMENT FACT SHEET
Vulnerability Scanning

DEFEND TODAY, SECURE TOMORROW

February 2022

OVERVIEW

CISA's Vulnerability Scanning (VS) is persistent "internet scanning-as-a-service" and part of CISA's service offerings. VS service continuously assesses the health of your internet-accessible assets by checking for known vulnerabilities, weak configurations—or configuration errors—and suboptimal security practices. VS service also recommends ways to enhance security through modern web and email standards.

VS service includes:

- **Target Discovery** identifies all active internet-accessible assets (networks, systems, and hosts) to be scanned.
- **Vulnerability Scanning** initiates non-intrusive checks to identify potential vulnerabilities and configuration weaknesses.

OBJECTIVES

- Maintain enterprise awareness of your internet-accessible systems.
- Provide insight into how systems and infrastructure appear to potential attackers.
- Drive proactive mitigation of vulnerabilities and reduce risk.

PHASES

Pre-Planning	Planning	Execution	Post-Execution
Stakeholder: • Requests service. • Provides target list (scope). • Signs and returns documents.	**CISA:** • Confirms scanning schedule. • Sends pre-scan notification to stakeholder.	**CISA:** • Performs initial scan of submitted scope. • Rescans scope based on detected vulnerability severity: ⇒ 12 hours for "critical" ⇒ 24 hours for "high" ⇒ 4 days for "medium" ⇒ 6 days for "low" ⇒ 7 days for "no vulnerabilities"	**CISA:** • Delivers weekly report to stakeholder. • Provides vulnerability mitigation recommendations to stakeholder. • Provides detailed findings in consumable format to stakeholder.

HOW TO GET STARTED

Contact vulnerability@cisa.dhs.gov to get started. Please keep in mind:

- CISA's assessments are available to both public and private organizations at no cost.
- Service availability is limited; service delivery timelines are available upon request. CISA prioritizes service delivery queues on a continuous basis to ensure no stakeholder/sector receives a disproportionate amount of resources and that the data collected is a diverse representation of the nation.

CISA | Assessments Service Request Form

Organization Name	Kenton County School District
Organization Customer Segment	State Government Entity
Organization Headquarters Address	1055 Eaton Drive Fort Wright Kentucky 41017 United States of America
Organization Assessment Point of Contact Name	Matthew Winkler
Organization Assessment Point of Contact Email	matthew.winkler@kenton.kyschools.us

Does this request include Election Infrastructure Systems? ○ Yes ● No

Which Critical Infrastructure Sector(s) does your organization most closely align with?

Government Facilities - Education Facilities

-

-

The North American Industry Classification System (NAICS) is the standard used by Federal statistical agencies in classifying business establishments for the purpose of collecting, analyzing, and publishing statistical data related to the U.S. business economy (How do I find my NAICS code?)

Please provide your organization's primary NAICS code: 611110

Please provide any additional NAICS codes associated with your organization:

Category of Assets/Networks to be assessed (select all the apply):

☑ Informational Technology (IT)

☑ Operational Technology (OT– ICS and SCADA)

□ Cloud Infrastructure (CI)

☑ Virtual Environment (VE)

Would your organization like to enroll in Cyber Hygiene Vulnerability Scanning?

Note: All services are available at no cost to federal agencies, state, local, tribal and territorial governments, critical infrastructure, and private organizations. Additional information can be found on the Cyber Resources Hub at cisa.gov/cyber-hygiene-services.

☑ Yes, we would like to enroll in Vulnerability Scanning

Organization Questions

The below questions are not required to receive Cyber Hygiene Vulnerability Scanning. CISA is collecting this information in order to tailor further service offerings to your organization and gain a better understanding of CISA's critical infrastructure partners.

How many employees are in your organization? Over 2,000

How many IT/ICS management and staff members are dedicated to your organization? 6 to 10

Does your organization have a dedicated Security Operations Center? Yes □ No ☑

Does your organization have the internal capability to respond to incidents? Yes ☑ No □

How does your organization allocate resources to cybersecurity? No formal budget is established

How many users in your organization utilize the networks you are hoping for CISA to assess? Over 1,000

How many customers does your organization serve? 18000

Is your organization seeking assessments in any of the below security areas?

☑ External and perimeter network configurations
☑ Security architecture
☑ Web application security
☑ Internal network configurations
□ Blue team and SOC capabilities
☑ Phishing prevention

If you selected OT (ICS/SCADA) on page 1, please answer the questions below: N/A ☑

Does your organization have current logical network diagrams? Yes ● No ○

Does your organization have managed network infrastructure devices (switch, router, firewall) at the IT/OT system demarcation points to facilitate header-only packet capture? Yes ● No ○

Does your organization have network admin staff that can use products such as Wireshark or T-shark to perform packet captures? Yes ● No ○

What are the predominant OT protocols (i.e. Modbus, DNP3, PROFIBUS and PROFINET, BACnet, etc.) in use?

Would you like to discuss the possibility of CISA working with your staff to facilitate network packet captures? Yes ● No ○

CYBER HYGIENE

Authorization to Conduct Continuous Scans of Public-Facing Networks and Systems

The Cybersecurity and Infrastructure Security Agency (CISA) of the Department of Homeland Security (DHS), under authority of Title XXII of the Homeland Security Act (6 U.S.C. § 651 et seq., esp. 6 U.S.C. § 659) would like to gain authorization from Kenton County School District (KCSD) to conduct continuous network and vulnerability scanning of KCSD's publicly accessible networks and systems.

The goals of these activities are to:

1. Catalog your organization's publicly accessible networks and systems, including services running and version/patch levels
2. Identify vulnerabilities on your organization's publicly accessible networks and systems
3. Identify potential configuration issues with your organization's public facing networks and systems
4. Maintain tactical awareness of the operational risks and cyber health of individual entities
5. Inform the government's common operational view of cyberspace
6. Integrate relevant information, analysis, and vulnerability assessments, in order to identify priorities for protective and support measures regarding potential or actual threats
7. Provide "early warning" of specific, actionable vulnerabilities to your organization

CISA activities will originate from IP addresses or other identifiers that will be made known to your organization.

Scanning will be openly attributable to the authorized scanning source, and should be detected by your organization's network monitoring solutions. Data will be sent to your organization's networks and systems corresponding to the public facing IP addresses, domain names, or other identifiers provided by your organization for scanning. The process has been designed to be as unobtrusive as possible: scheduling, intensity and frequency have been carefully planned to minimize the possibility of service disruption.

Activities under this authorization will be limited to scanning; no attempts to connect to your organization's internal network, penetrate your organization's systems, or monitor your organization's network traffic will be made under this authorization.

If a third-party, such as a cloud service provider, operates or maintains your networks or systems to be scanned pursuant to this authorization, your organization will ensure compliance with any notification or authorization requirement that such third party may impose on external vulnerability scanning services. If your organization is informed that any such third party prohibits external vulnerability scans, you will promptly notify the CISA point of contact listed below.

In a separate appendix to this authorization please provide the following information: the point of contact for activities performed under this authorization; an email address for the delivery of reports; identification information for your organization's networks and systems to be scanned pursuant to this authorization; and any other relevant information. Your organization may provide updates to this information from time to time, in writing, using an updated appendix or other method. Your organization must promptly update CISA of changes to the identifying information used to scan your networks and systems pursuant to this authorization.

CISA acknowledges that this authorization may be withdrawn at any time for any reason.

The CISA Point of Contact for this activity can be reached at vulnerability_info@cisa.dhs.gov. All notifications, updates, or other communications regarding this authorization and any related activity should be sent to this CISA Point of Contact.

By signing below, you agree to the following:

- You have authority to authorize scanning of the networks and systems submitted pursuant to this authorization;
- You authorize CISA to conduct the scanning activities described above;
- You agree to promptly update CISA of changes to the information used to identify the networks and systems to be scanned pursuant to this authorization;
- You agree to comply with any notification or authorization requirement that any third-party that operates or maintains your networks or systems may impose on external vulnerability scanning services, notifying CISA if external scanning is later prohibited;
- You accept that, while CISA teams will use their best efforts to conduct scans in a way that minimizes risk to your organization's systems and networks, the scanning activities described above create some risk of degradation in performance to your organization's systems and networks;
- You acknowledge that CISA provides no warranties of any kind relating to any aspect of the assistance provided under this authorization; and
- You are authorized to make the above certifications on your organization's behalf.

Signature: Matthew Winkler Digitally signed by Matthew Winkler
Date: 2024.04.23 08:38:28 -04'00'

Name: Matthew Winkler **Date:** 04/23/2024

Title: Director of Technology

Email: matthew.winkler@kenton.kyschools.us **Phone:** 859.957.2612

Entity: Kenton County School District

City: Fort Wright **County:** Kenton **State:** KY

Country: United States of America

Appendix A

Authorization to Conduct Continuous Scans of Public-Facing Networks and Systems

KCSD *provides the following information to facilitate the authorized scanning activities:*

Please provide a **technical point of contact** at KCSD for the CISA team to follow-up with:

Name: Matthew Winkler

Email: matthew.winkler@kenton.kyschools.us

Phone: 859.957.2612

Optional secondary **technical point of contact**:

Name: Gary Crawford

Email: gary.crawford@kenton.kyschools.us

Phone: 859.322.6142

We recommend your organization **create/use a distribution list** email address to receive our reports. This allows your organization to manage the recipients of our report. *We will only deliver reports to a single address.*

Distro email: matthew.winkler@kenton.kyschools.us

Your report will be encrypted with a password which we will provide to you. **How would you like this password delivered** (select one)?

Email @

☑ Tech POC
□ Distro POC

When should scans begin? (e.g., as soon as possible, or *time*, Eastern @ *mm/dd/yyyy*)

As soon as possible

Identification of Your Public-Facing Networks and Systems:

Enter your organization's **internet-facing, static IPv4 addresses** to be vulnerability scanned in one of the following formats: CIDR notation (e.g. x.x.x.0/24), IP range (e.g. x.x.x.1-x.x.x.200), or individual IPs (e.g. x.x.x.1) with one entry per line:

170.185.126.0/24
170.185.127.0/24