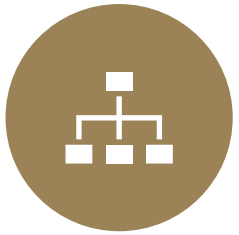
Technology Committee

MONDAY, DECEMBER 11 , 2023

INFRASTRUCTURE

CYBER SECURITY



DEPARTMENT

NO UPDATES

WEBSITE

CIS CONTROLS

Infrastructure

Previous meeting

Session Initiation Protocol (SIP) trunk has been installed; we are scheduling the gateway installations.

Updates

- SIP trunk will be turned on December 13, 2023.
- Faculty Chromebooks have been deployed.
- Grades 9-10 chromebooks have been swapped out.
- Grade 11 to be done after Winter Break.
- Grade 12 TBA.

Cyber Security Updates

Previous meeting

- Cores switches have not been installed yet, waiting on schedule.
- ACL Access Control Lists will be configured with core switch installation.
- Antoinette King, founder of Credo Cyber will be speaking at the November 22 Superintendent Conference Day.

Update

- Core switches are racked, and we will be cutover on January 10, 2024
- ACL are configured and applied, currently troubleshooting some issues.
- Met with CISA (Cybersecurity Infrastructure Security Agency) to discuss services available to District.

****Cyber Security work is an ongoing process imbedded in our daily activities.**

CIS Controls®
Version 8

CIS Control 6 – Users – Account Control Management

Account Control Management Use processes and tools to assign and manage authorization to credentials for user accounts, including administrator accounts, as well as service accounts, to enterprise assets and software

Control 6.1 - Establish an Access Granting Process (NIST PR.AC-1) • Establish and follow a process, preferably automated, for granting access to enterprise assets upon new hire, rights grant, or role change of a user.

-Practices are in place for user account creation and removal. Accounts are only added/removed upon email request from the Superintendent Office or any of the Asst Superintendent's Offices.

Student accounts are automated through Schooltool.

CIS Controls®
Version 8

Control 6.2 - Establish an Access Revoking Process

Control 6.2 - Establish and follow a process, preferably automated, for revoking access to enterprise assets, through disabling accounts immediately upon termination, rights revocation, or role change of a user. Disabling accounts, instead of deleting accounts, may be necessary to preserve audit trails.

-Practices are in place for user account creation and removal. Accounts are only added/removed upon email request from the Superintendent Office or any of the Asst Superintendent's Offices.

Student accounts are automated through Schooltool.

CIS Controls®
Version 8

Control 6.3 - Require MFA for Externally Exposed Applications (NIST PR.AC-7) • Require all externally-exposed enterprise or third-party applications to enforce MFA, where supported. Enforcing MFA through a directory service or SSO provider is a satisfactory implementation of this safeguard.

Control 6.4 - Require MFA for Remote Network Access (NIST PR.AC-7, PR.AC-3) • Require MFA for remote network access.

Control 6.5 - Require MFA for Administrative Access (NIST PR.AC-7) • Require MFA for all administrative access accounts, where supported, on all enterprise assets, whether managed on-site or through a third-party provider

MFA is required for all Faculty/Staff when accessing District resources from outside the district.

Antoinette King, Founder of Credo Cyber, Guest Speaker at Superintendents Conference Day.

Antoinette King discussed the following topics:

- Why is Cybersecurity Important?
- Data Types
- Trends in K-12 Threat Landscape
- Impacts of a Data Breach
- Data Privacy Responsibilities
- Cyber Hygiene Best Practices

Who Are they:

- Part of DHS Department of Homeland Security
- Works with partners to defend against today's threats and collaborate to build a more secure and resilient infrastructure for the future.

What they offer us:

- Vulnerability Scanning
- TTX, Tabletop Exercises
- Assessments services.

Wallkill/BOCES are working on a 3 county TTX in the spring.

CISA Tabletop Exercise Packages (CTEPs) are a comprehensive set of resources designed to assist stakeholders in conducting their own exercises. Partners can use CTEPs to initiate discussions within their organizations about their ability to address a variety of threat scenarios.

Cybersecurity Scenarios

These CTEPs include cybersecurity-based scenarios that incorporate various cyber threat vectors including ransomware, insider threats, phishing, and Industrial Control System (ICS) compromise. There are also sector-specific cybersecurity scenarios for elections infrastructure, local governments, maritime ports, water, and healthcare.

Cyber-Physical Convergence Scenarios

Physical impacts resulting from a cyber threat vector, or cyber impacts resulting from a physical threat vector. While CTEPs within the cyber and physical sections may touch on these subjects, convergence CTEPs are designed to further explore the impacts of convergence and how to enhance one's resiliency.

**Wallkill will be subscribing to CISA free vulnerability scan.

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.

Website

REMINDER:

WEBSITE WILL NEED TO BE MIGRATED TO THE NEW PLATFORM BY JANUARY 2025.

https://www.finalsite.com/conversion-themes

We will create a timeline to prepare for the conversion in fall of 2024.