January Technology Board Report - Cybersecurity Update

Multi Factor Authentication Enabled: Lindsay Greenbergand I tested and implemented Google Single Sign On for PowerSchool. This leverages the strength of Google MFA, that we already have in place, to secure our SIS. It also means one less password for Staff and Students to remember. (Yeah!) We gave people a heads up on Friday, turned it on over the weekend, and had no questions on Monday AM.

Data Governance Plan:
This document has been completed and is ready for 1st reading. It was in draft form since 2019. Please feel free to use the Comment Feature in Google Docs if you have feedback or questions!

SAU 50 Data Governance Manual -2023

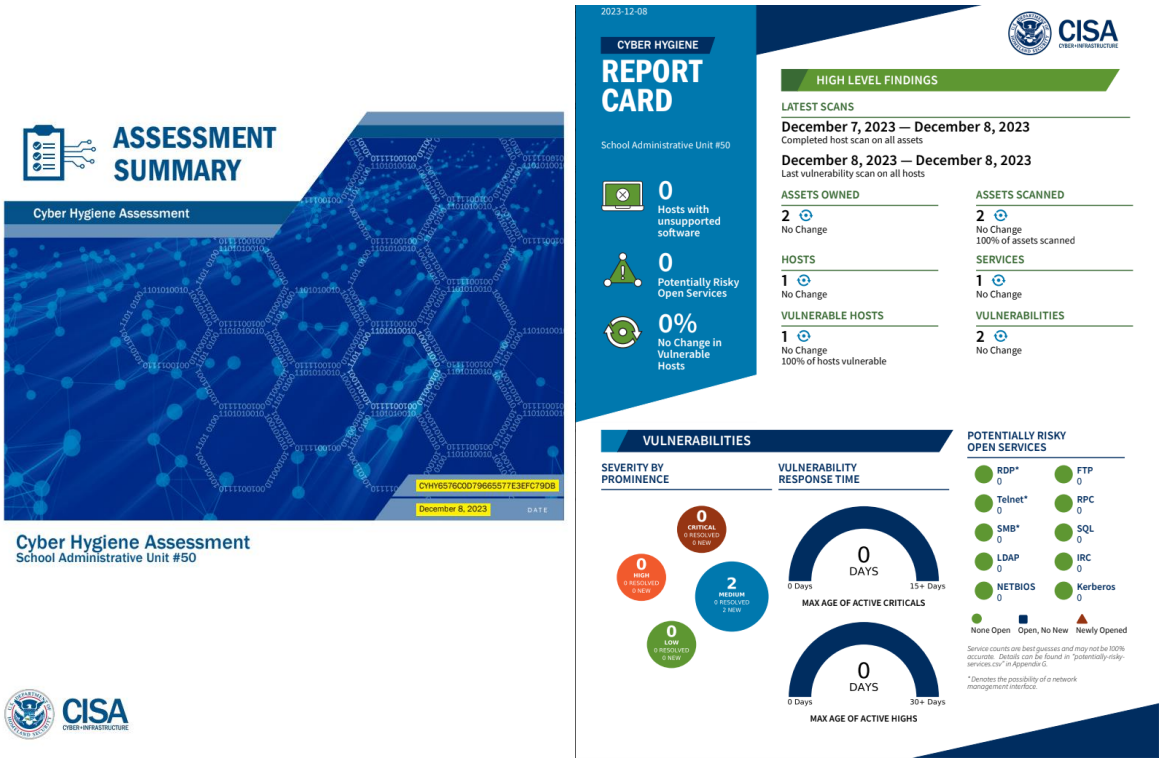
Partnerships with Federal Agencies

CISA - Cybersecurity & Infrastructure Security Agency - The Cybersecurity and Infrastructure Security Agency (CISA) is an operational component of the Department of Homeland Security (DHS). CISA works to understand, manage, and mitigate risk to the nation's cyber and physical infrastructure in the public and private sector.

MS-ISAC - The Multi-State Information Sharing and Analysis Center (MS-ISAC) is a CISA-supported collaboration with the Center for Internet Security designed to serve as the central cybersecurity resource for the nation's State, Local, Territorial, Tribal (SLTT) governments. MS-ISAC releases weekly updates on current threats and vulnerabilities.

Cybersecurity Assessments

CISA Cyber Hygiene Assessment: Ongoing Scanning of Public facing systems to look for network vulnerabilities. Started in December. Reports arrive via email weekly, with any vulnerabilities highlighted.



CISA Ransomware Readiness Assessment: New service offered by NH CISA. SAU 50 introductory call has been scheduled.

CIS FRAMEWORKS-

MacOS Controls:
CIS_Apple_macOS_14.0_Sonoma_v1.0.0.pdf Process of Review underway for MacOS Sonoma, which is currently released. SAU 50 Staff Devices will be updated in Spring '24.

Critical Security Controls - Version 8:

Introduction

The CIS Critical Security Controls® (CIS Controls®) started as a simple grassroots activity to identify the most common and important real-world cyber-attacks that affect enterprises every day, translate that knowledge and experience into positive, constructive action for defenders, and then share that information with a wider audience. The original goals were modest—to help people and enterprises focus their attention and get started on the most important steps to defend themselves from the attacks that really mattered.

Led by the Center for Internet Security® (CIS®), the CIS Controls have matured into an international community of volunteer individuals and institutions that:

- Share insights into attacks and attackers, identify root causes, and translate that into classes of defensive action
- Create and share tools, working aids, and stories of adoption and problem-solving
- Map the CIS Controls to regulatory and compliance frameworks in order to ensure alignment and bring collective priority and focus to them
- Identify common problems and barriers (like initial assessment and implementation roadmaps), and solve them as a community

The CIS Controls reflect the combined knowledge of experts from every part of the ecosystem (companies, governments, individuals), with every role (threat responders and analysts, technologists, information technology (IT) operators and defenders, vulnerability-finders, tool makers, solution providers, users, policy-makers, auditors, etc.), and across many sectors (government, power, defense, finance, transportation, academia, consulting, security, IT, etc.), who have banded together to create, adopt, and support the CIS Controls.

CIS_Controls__v8__Critical_Security_Controls__2023_08.pdf

“Whether you use the CIS Controls, and/or another way to guide your security improvement program, you should recognize that “it’s not about the list.” You can get a credible list of security recommendations from many sources—it is best to think of the list as a starting point. It is important to look for the ecosystem that grows up around the list.” - ***CIS Critical Security Controls- Version 8.***

References - For More information about CISA and K-12 please see their annual report from 2023. Click the Image for link.

KEY FINDINGS

AND RECOMMENDATIONS

	FINDING	RECOMMENDATION
01	**With finite resources, K–12 institutions can take a small number of steps to significantly reduce cybersecurity risk.**	**Invest in the most impactful security measures and build toward a mature cybersecurity plan** by taking these three steps: • Implement highest priority security controls. • Prioritize further near-term investments in alignment with the full list of CISA's Cross-Sector Cybersecurity Performance Goals (CPGs). • Over the long-term, develop a unique cybersecurity plan that leverages the NIST Cybersecurity Framework (CSF).
02	**Many school districts struggle with insufficient IT resources and cybersecurity capacity.**	**Recognize and actively address resource constraints**: • Work with the state planning committee to leverage the State and Local Cybersecurity Grant Program (SLCGP). • Utilize free or low-cost services to make near-term improvements in resource-constrained environments. • Expect and call for technology providers to enable strong security controls by default for no additional charge. • Minimize the burden of security by migrating IT services to more secure cloud versions.
03	**No K–12 entity can singlehandedly identify and prioritize emerging threats, vulnerabilities, and risks.**	**Focus on collaboration and information sharing**: • Join relevant collaboration groups, such as MS-ISAC and K12 SIX. • Work with other information-sharing organizations, such as fusion centers, state school safety centers, other state and regional agencies, and associations. • Build a strong and enduring relationship with CISA and FBI regional cybersecurity personnel.

Cyber Security Incident Response Plan -

We have developed a SAU50 Cyber-Security Incident Response Plan as part of our larger SAU 50 Data Governance Manual -2023 Manual- DRAFT.. . The IRP defines the Who, What, Where, Why and How of the SAU 50 Response to any one of the common categories of cyber incidents. - Appendix B.

Appendix B - Incident Categorization

COMMON CATEGORIES OF CYBER INCIDENTS

Incident Type	Type Description
Unauthorized Access	When an individual or entity gains logical or physical access without permission to a company network, system, application, data, or other resource.
Denial of Service (DoS, DDoS)	An attack that successfully prevents or impairs the normal authorized functionality of networks, systems, or applications by exhausting resources.
Malicious Code	Successful installation of malicious software (e.g., a virus, worm, Trojan horse, or other code-based malicious entity) that infects an operating system or application.
Improper or Inappropriate Usage	When a person violates acceptable computing policies, including unauthorized access or data theft.
Suspected PII Breach	An incident where it is suspected that Personally Identifiable Information (PII) has been accessed.
Suspected loss of Sensitive Information	An incident that involves a suspected loss of sensitive information (not PII) that occurred because of Unauthorized Access, Malicious Code, or Improper (or Inappropriate) use, where the cause or extent is not known.

New Hampshire Department of Education
Guidance on Acceptable Security Certifications in lieu of the Minimum Standards under RSA 189:66

New Hampshire
Department of Education

The purpose of this guidance is to provide acknowledgement and recognition of national or international security assessment and certification standards which meet or exceed the New Hampshire "Minimum Standards for Privacy and Security of Student and Employee Data," as established under RSA 189:66, and may be accepted by Districts in lieu of a specific assessment against the Minimum Standards.

It should further be noted that the list of acceptable security standards may not match up one for one with the Minimum Standards, however all of the national or international security standards listed below either meet or exceed the Minimum Standards in depth and/or breadth, and demonstrate sufficient rigor in applying security and privacy requirements to their respective software application, digital tool, extension or online service.

Therefore, the Department of Education considers that applications or services that can demonstrate successful completion of the following national or international security assessments, authorizations or certifications as meeting or exceeding the Minimum Standards as established under RSA 189:66, and may be accepted by Districts in lieu of a specific assessment against the Minimum Standards:

- NIST SP 800-171 rev 2, Basic and Derived Requirements
- NIST SP 800-53 rev 4 or newer, Low Impact Baseline or higher
- FedRAMP (Federal Risk and Authorization Management Program)
- ISO/IEC 27001:2013
- Center for Internet Security (CIS) Controls, v. 7.1, Implementation Group 1 or higher
- AICPA System and Organization Controls (SOC) 2, Type 2
- Payment Card Industry Data Security Standard (PCI DSS), v3.2.1

Evidence of successful certification based on the preceding security standards could be in the form of a national or international Certification document; an Authorization to Operate (ATO) issued by a state or federal agency, or by a recognized security standards body; or a Preliminary Authorization to Operate (P-ATO) issued by the FedRAMP Joint Authorization Board (JAB).