Cybersecurity Resource Recommendations

The Federal Communications Commission (FCC) is launching the Schools and Libraries Cybersecurity Pilot Program to provide up to $200 million to selected schools and libraries to defray the costs of cybersecurity equipment and services. Given the critical importance of strong cybersecurity protections for K-12 schools' and libraries' networks, the FCC, in consultation with the Cybersecurity and Infrastructure Security Agency (CISA) and the Department of Education (ED), provide the following cybersecurity guidance and recommended resources to help keep networks and data safe. We recognize that schools and libraries often face budget and resource constraints, so these recommendations highlight free and low-cost options and focus on the most impactful initial steps. The Cybersecurity Pilot Program offers flexibility to allow each potential applicant to structure its request based on its unique needs and these resources are intended to serve as a guide for possible procurement approaches.

Which risks should I focus on first? Schools and libraries should consider the most common ways malicious cyber actors exploit technology to gain access to networks as identified in the joint CISA/ED K-12 Critical Infrastructure Brief: Defensible and Resilient. These include:

What are the most impactful solutions? Schools and libraries should first focus their resources by implementing the highest priority security measures identified in ED's Cybersecurity Action Steps for the K-12 Community or CISA's Report: Partnering to Safeguard K-12 Organizations from Cybersecurity Threats. Recommendations include:

Second, schools and libraries should look for technology vendors that prioritize security from the earliest stages of development to ensure the products they deliver are secure against attackers by design and by default. Examples include secure authentication enabled by default, actions taken to prevent or reduce common vulnerabilities before customer deployment, and enabling customers to gather evidence of intrusions at no cost.

What resources are available? We recommend that schools and libraries consider free and low-cost resources, including:

- CISA's **Cyber Hygiene Vulnerability Scanning Services**, which continuously assesses the health of a district's internet-accessible assets by checking for known vulnerabilities and weak configurations and then recommends ways to enhance your security.
- **Protective Domain Name Service (PDNS)**, which prevents access to domains known to be malicious. There are a variety of technology companies and other service providers that can provide PDNS to schools. One provider is the Federal government-funded Multi-State Information Sharing and Analysis Center (MS-ISAC), which offers PDNS to schools for no-cost through its Malicious Domain Blocking and Reporting (MDBR) service.

Data breaches and ransomware together comprised ~80% of publicly disclosed K-12 cyber incidents in the United States in 2022; moreover, in 85% of those breaches the technology vendor was at fault.[1] Stolen credentials from breached software databases, combined with a lack of secure authentication, is a recipe for ransomware and identity theft disaster. We encourage schools and libraries to use CISA's Secure by Demand Guide and ask vendors about their products' security when completing procurements to ensure they prioritize security and implement cybersecurity best practices.

My school, library, or consortium may want to explore the following eligible services if applying to the Cybersecurity Pilot Program:	**My school, library, or consortium should look for software and security products that:**
• Multi-Factor Authentication (MFA) and Implementation Support, starting first with the most critical systems and accounts, to prevent unauthorized access • Single Sign-On to enhance security and user experience across applications • Advanced/Next-Generation Firewalls • Advanced Attack Surface Management and Asset Management Solutions to easily maintain IT inventory • Endpoint Detection & Response (EDR) to quickly identify a breach and notify administrators • Offsite/Immutable Backups to enable restoration in the event of an incident • Network segmentation to improve control • Automated Patch management solutions to protect against vulnerabilities • Data Loss Prevention tools to detect potential breaches	• Enable (phishing-resistant) MFA by default or integrate Single Sign-On by default and at no cost • Do not contain default or hard-coded passwords • Make it simple and free for customers to install security patches and offer support for technology end-of-life • Make security logs available to customers in the baseline version • Do not contain common product defects that attackers consistently and easily exploit, or, at a minimum, have roadmaps that highlight how the vendor plans to eliminate such classes of defect • Support a Vulnerability Disclosure Policy for security researchers

[1] Keynote from Doug Levin, Director, K12 Security Information eXchange (K12 SIX), *The State of K-12 Cybersecurity: Year in Review*, The 2023 National K-12 Cybersecurity Leadership Conference, Austin, TX (Feb. 22-23, 2023).