KEY FINDINGS
AND RECOMMENDATIONS

01

FINDING	RECOMMENDATION
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

FINDING	RECOMMENDATION
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

FINDING	RECOMMENDATION
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.