KEY FINDINGS

01

In an environment of limited resources, leaders should leverage security investments to focus on the most impactful steps. K–12 entities should begin with a small number of prioritized investments: deploying multi-factor authentication (MFA), mitigating known exploited vulnerabilities, implementing and testing backups, regularly exercising an incident response plan, and implementing a strong cybersecurity training program. K–12 entities should then progress to fully adopting CISA's Cybersecurity Performance Goals (CPGs) and mature to building an enterprise cyber-security plan aligned around the NIST Cybersecurity Framework (CSF).

02

Cybersecurity risk management must be elevated as a top priority for administrators, superintendents, and other leaders at every K–12 institution. Leaders must take creative approaches to securing necessary resources, including leveraging available grant programs, working with technology providers to benefit from low-cost services and products that are secure by design and default, and urgently reducing the security burden by migrating to secure cloud environments and trusted managed services.

03

No K–12 institution is an island. Information sharing and collaboration with peers and partners is essential to build awareness and sustain resilience. K–12 entities should participate in an information sharing forum such as the Multi-State Information Sharing and Analysis Center (MS-ISAC) and/or K12 Security Information eXchange (K12 SIX) and establish a relationship with CISA and FBI field personnel.