Nicole Galloway, CPA
Missouri State Auditor

CITIZENS SUMMARY

Findings in the Cyber Aware Schools Audit of the Boonville R-1 School District

Background	The Boonville R-1 School District's Student Data Governance Audit was completed as part of the Cyber Aware School Audits Initiative. These audits are designed to assess the effectiveness of privacy and security controls with a focus on identifying practices to improve the security of information school districts have on students and their families. The district uses a student information system (SIS) to maintain student data and to track and monitor academic progress. The SIS maintains private and confidential data, such as social security numbers and assessment test scores. Additional systems and applications that maintain data are used for administrative functions and to enhance student productivity and classroom collaboration. The district relies extensively on computerized systems to support its educational and mission-related operations and on information security controls to protect the sensitive data residing on those systems. Auditors identified areas where improvements are needed but also found the district has developed certain controls to establish a safe environment for using technology, including promoting online safety, security, and confidentiality.
Data Governance	The district has not established a comprehensive data governance program, a critical task for any educational organization. A comprehensive program is necessary to ensure the confidentiality, integrity, availability, and quality of data. Without a formal program, the district cannot ensure that personally identifiable information (PII) is adequately protected and safe from unauthorized access, misuse, or inadvertent disclosure.
Security Controls	The district has not implemented necessary security controls, leaving technology assets, including PII, at risk of inappropriate access, use, and disclosure. The district has not formally appointed any specific personnel to serve as security administrator or formally assigned responsibility for creating, implementing, and maintaining security policies and procedures. Without documented and approved policies and procedures, management lacks assurance that security controls are appropriate and properly applied.
User Accounts	The district has not fully established controls for creating and maintaining user accounts for accessing system resources. Control activities range from requesting and establishing accounts to suspending or closing accounts. Additionally, periodic review of accounts and privileges is necessary to promote data security. Policies and procedures for maintaining user access to data and other system resources are not fully documented, and periodic reviews of users' privileges to ensure access remains aligned with job duties are not performed. Without appropriate account access policies and procedures, including periodically reviewing user access rights, users may be granted inappropriate or unauthorized access, which can provide opportunities for misuse or inappropriate disclosure of sensitive data.
Incident Response and Continuity Planning	The district has not taken all necessary measures to protect data in the event of a breach or other disruptive incident. The district has not formally documented policies and procedures for responding to security incidents, has not adopted a formal data breach response policy, and has not fully documented and tested a continuity plan. Without comprehensive incident response and breach-related policies, management may not be sufficiently

equipped to respond quickly and effectively to an incident or breach, increasing the risk of potential harm to the district or affected individuals. Without a tested and functional continuity plan, management has limited assurance the organization's business functions and computer processing can be sustained during or promptly resumed after a disruptive incident.

Security Awareness Program	The district has not established a formal security and privacy awareness training program. As education organizations implement more powerful information systems and become more reliant on electronic data, proactive security awareness programs become increasingly important. With proper security and privacy awareness training and clear communication of data and device use policies, employees can become the first line of defense against cybersecurity incidents. However, without adequate training, users may not understand system security risks and their role in implementing related policies and controls to mitigate those risks.
Vendor Monitoring	The district has not established a process for ensuring software acquired or outsourced from information technology vendors complies with data security principles. Additionally, the district cannot locate a written contract with the vendor of one of its key systems. Without an effective process for monitoring and managing risk of software acquisition or outsourcing, the district has less assurance in a vendor's ability to deliver services effectively, securely, and reliably and to ensure that services meet current and future data privacy and security needs.

Because of the nature of this report, no overall rating is provided.

All reports are available on our Web site: auditor.mo.gov