September 2016

Nicole Galloway, CPA
Missouri State Auditor

CITIZENS SUMMARY

Findings in the Cyber Aware School Audit of the Park Hill School District

Background

The Park Hill 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 assessment test scores and other sensitive data. 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.

User Accounts

The district has not fully established controls for maintaining user accounts for accessing system resources. While certain procedures for removing access are in place, the district has not documented or fully established policies and procedures for disabling or removing user accounts timely after a user terminates. As of June 2016, three former district employees still had access to district systems and information 30 or more days after leaving the district. In addition, the district does not proactively monitor for student information system user accounts that have not been accessed or used for a specified period of time.

Security Controls

The district has not implemented all necessary security controls, leaving technology assets, including personally identifiable information, 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. Additionally, the district has not established adequate password controls to reduce the risk of unauthorized access to computers and data. Without documented and approved policies and procedures, management lacks assurance that security controls are appropriate and properly applied.

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

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