Office of the State Auditor

Kerri L. Hunter, CPA, CFE
State Auditor

FOR IMMEDIATE RELEASE

Contact: Greg Fugate
osa.media@coleg.gov

June 12, 2023

State Audit Finds that Improved Governance and Oversight Are Needed for Security of State Systems

DENVER—The Colorado Office of the State Auditor (OSA) has issued a performance audit of cybersecurity resiliency at the Governor's Office of Information Technology (OIT). By statute, OIT is the State's centralized information technology department responsible for managing information technology resources and staff for most Executive Branch agencies, known as consolidated agencies.

Overall, the audit, which was performed by a third party under contract with the OSA, found that ambiguity about OIT's statewide security roles and responsibilities has led to inconsistencies in the implementation of security practices and confusion about who is responsible for the execution of security control activities between OIT, consolidated agencies, and third-party vendors. For example, OIT had not consistently defined who or what constitutes a "business owner," using the term haphazardly throughout many of its policies, procedures, and other formal documents. OIT also had not differentiated between enterprise-level, agency-level, and system-level ownership when referring to the business owner, leading to confusion about who is responsible or how a control is applied. Auditors found that business owners (individuals) were not formally identified for a population of 384 applications managed by OIT, including 73 critical and essential systems. Where business owners (individuals) had been identified by OIT, auditors' examination of system security plans, inspection of system inventories, and interviews with personnel at both OIT and consolidated agencies revealed inaccuracies and inconsistencies in who was acknowledged as the actual business owner.

Auditors also found that OIT needs more effective analysis and coordination to prioritize its list of more than 200 critical and essential systems across all consolidated agencies. Having a clear understanding of cross-agency priorities would serve to focus and improve all aspects of OIT's responsibilities and service delivery, including fundamental security and operational activities such as planning and executing disaster recovery, responding to incidents, patching and updating systems, resolving helpdesk tickets, conducting risk assessments, and developing system security plans.

Auditors also found that OIT had not effectively communicated the release of updated security policies to those who were responsible for their implementation and execution, nor had OIT provided role-based security training to all information security personnel. For example, auditors interviewed leadership at a selection of five consolidated agencies who confirmed that none of their personnel responsible for information security activities had ever received training or instruction on their security roles and responsibilities as business owners. Additionally, auditors tested employees and external users across five consolidated agencies and OIT and found that 4 of 24 (17 percent) employees tested and 14 of 18 (78 percent) external users tested had not completed quarterly security training in a timely manner. Two of three OIT contractors tested had not completed any type of security awareness training.

"This cybersecurity resiliency audit provides OIT with important action items to address security gaps and help ensure the reliability and protection of the State's critical information systems and data," said Cindi Radke, Legislative Audit Manager.

The public audit report makes two recommendations to OIT for improvements and is available online at www.colorado.gov/auditor.

The audit had 10 additional confidential findings for OIT; however, the details of these findings were kept confidential and not publicly released by the Legislative Audit Committee due to their security-sensitive nature.

About the Office of the State Auditor

Under the direction of the State Auditor, the OSA's nonpartisan, professional staff promote government accountability by conducting independent performance, financial, and IT audits and evaluations of state agencies, departments, and institutions of higher education; conducting independent evaluations of the State's tax expenditures (e.g., credits, exemptions, deductions); tracking about 4,000 Colorado local governments for compliance with the Local Government Audit Law; and operating a statewide fraud reporting hotline.

###