Report Highlights

Cybersecurity Resiliency

Governor's Office of Information Technology

IT Performance Audit • January 2026 • 2551P-IT

OFFICE OF THE STATE AUDITOR
COLORADO

Key Concerns

The Governor's Office of Information Technology (OIT), as of June 30, 2025, had not fully implemented our May 2023 Audit of Cybersecurity Resiliency at OIT (Public Report) recommendations in the areas of IT Governance and Information Security Training and Awareness.

Additionally, OIT did not fully implement our May 2023 confidential audit report recommendations in the IT areas of Asset Management, Contingency Planning, Identification and Authentication, Incident Response, Logging and Monitoring, Physical Access, Risk Management, Security Planning, User Access Management, and Vulnerability and Patch Management.

Of the 71 prior recommendations that we performed follow-up testwork on as part of this audit, we determined that OIT had:

- **Implemented** 10 recommendations (14 percent)
- **Partially Implemented** 53 recommendations (75 percent)
- **Not Implemented** 8 recommendations (11 percent)

Without fully addressing our prior cybersecurity resiliency recommendations, OIT may not be able to fully meet its statutory responsibilities to ensure that information that Colorado's citizens have entrusted to state agencies is safe, secure and protected from unauthorized access, unauthorized use, or destruction [Section 24-37.5-401(b), C.R.S.].

Key Findings

- **IT Governance:** OIT did not provide sufficient documentation to demonstrate that it coordinated with state agency staff on its new process for system classifications that are based on how important the system's availability is to the agency's mission. In addition, OIT did not respond to inquiries made during the audit to clarify whether it was attempting to transfer its statutory authority to the various state agencies for ensuring their compliance with security policies and conducting information security audits and assessments. Specifically, OIT's December 2024 Colorado Information Security Policies (CISP) required various state agencies to be "responsible for contracting for security and compliance and that there is a validation of compliance." Additionally, OIT did not provide sufficient documentation that its Technical Standards had been updated and approved by OIT management and that the Technical Standards consistently established minimum security requirements.

- **Information Security Training and Awareness:** OIT indicated that it does not plan to provide training to state agency staff on their security responsibilities, even though it agreed to do so at the time of the May 2023 audit, and even though OIT's December 2024 CISPs assign security responsibilities to agency staff. Further, OIT indicates that it does not plan to provide training to its IT Director staff who support agency staff in conducting their IT-related responsibilities, even though OIT has also assigned them security responsibilities on which the IT Directors should be trained. OIT also failed to provide sufficient documentation that it assessed sanctions on its staff, as required by OIT's Business Operating Procedure for Noncompliance with Required Training, for their noncompliance with training and Acceptable Use Policy requirements.

Due to the sensitive nature of additional findings we identified through our follow-up audit—Findings 3 through 12—those detailed findings have been included in a separate, confidential report and provided to OIT.

Background

- OIT is the State's centralized IT department responsible for managing IT service delivery and resources, including personnel and equipment, for state agencies that have been consolidated under statute [Section 24-37.5-105, C.R.S.], as of July 1, 2008.

- The Chief Information Officer (CIO) is the state executive who leads OIT and is ultimately responsible for the security of state systems and information [Section 24-37.5-106, C.R.S.].

- The Chief Information Security Officer (CISO) reports to the CIO and serves as the point of contact for all information security matters in the State of Colorado. The CISO is responsible for informing the CIO and executive agency leadership of security risks and the impacts of policy and management decisions on IT-related initiatives [Section 24-37.5-403, C.R.S.].

- State agencies, also referred to as "consolidated agencies," are all of the departments, divisions, commissions, boards, bureaus, and institutions in the Executive Branch of the state government except for the following, which are referred to as "non-consolidated" agencies—Legislative Branch agencies; Judicial Branch agencies; the Departments of Education, Law, State, and Treasury; and state-supported institutions of higher education.

Audit Recommendations Made	Agency Responses		
	Agree	Partially Agree	Disagree
85	18	30	37