REPORT HIGHLIGHTS

Audit of Cybersecurity Resiliency at the Governor's Office of Information Technology
IT Performance Audit, May 2023 – Report Number 2250P-IT

AUDIT CONCERNS

Audits that conclude on an organization's cybersecurity resiliency, can improve their ability to prevent, detect, and respond to cyber threats, which helps to minimize the risk and potential impact of security breaches, which in turn would increase the integrity of information systems and the associated data. Evaluating and improving the State's cybersecurity posture directly relates to the Colorado General Assembly's determination and declaration established in Section 24-37.5-401, C.R.S. Specifically, the General Assembly stated that the state government has a duty to the Colorado's citizens to ensure that information the citizens have entrusted to public agencies is safe, secure, and protected from unauthorized access, unauthorized use, or destruction [Section 24.37.5-401(b)].

By statute, the Governor's Office of Information Technology (OIT) is responsible for delivery of information technology to State agencies, including the oversight and direction of information security, as well as ensuring that State agencies within the Executive Branch have established resilient cybersecurity practices and proper internal controls to identify, prevent, and detect cyber threats. This public report identifies the following main concerns:

- OIT has not clearly defined state-wide security roles and responsibilities to align with those same responsibilities outlined in Colorado Revised Statutes. This ambiguity has led to inconsistencies in the implementation of security practices and confusion on who is responsible for execution of security control activities – either OIT, an agency, or 3rd party vendor.
- OIT recently updated the Colorado Information Security Policies (CISPs) without proper education and planning to all affected parties. This lack of education has exacerbated the security roles and responsibilities issue as these updated policies migrated significant responsibilities from OIT to agencies.

Additional concerns were identified related to the areas of Asset Management, Contingency Planning, Identification and Authentication, Incident Response, Logging and Monitoring, Physical Access Controls, Risk Management, Security Planning, User Account Management, and Vulnerability and Patch Management. Due to the sensitive nature of these concerns, the details have been included in a separate, confidential report, as Findings 3 through 12.

BACKGROUND

The Governor's Office of Information Technology

- OIT is the State's centralized information technology department responsible for managing information technology resources and staff for all consolidated agencies.
- OIT is responsible for maintaining the State's IT Security Program and managing the CISPs.

KEY FACTS AND FINDINGS

- OIT had not clearly defined OIT’s security roles and responsibilities to align with those outlined in Colorado Revised Statutes.
- OIT had not established an effective and holistic approach for the prioritization of information systems across the State’s IT enterprise.
- OIT had not effectively communicated the release of updated security policies to those who were responsible for their implementation and execution.
- OIT had not established minimum security requirements for key security activities.

Additional key facts and findings were identified related to the areas of Asset Management, Contingency Planning, Identification and Authentication, Incident Response, Logging and Monitoring, Physical Access Controls, Risk Management, Security Planning, User Account Management, and Vulnerability and Patch Management. Due to the sensitive nature of these key facts and findings, they have been included in a separate, confidential report, as Findings 3 through 12.

The box below provides a count of the total recommendations made from this audit, including those in both the public report and the associated confidential report. This box also provides a count of the number of recommendations with which OIT management agreed, partially agreed, or disagreed.

Recommendations Made

77

Responses

Agree: **56**

Partially Agree: **16**

Disagree: **5**