



November 22, 2024

## **Audit of Cybersecurity Resiliency at the Governor's Office of Information Technology – Public Status Report**

Members of the Legislative Audit Committee:

Attached is the status report from the Governor's Office of Information Technology (OIT) on the implementation of recommendations contained in the Office of the State Auditor's (OSA) *Audit of Cybersecurity Resiliency at the Governor's Office of Information Technology – Public Report*. At the December 9, 2024, Legislative Audit Committee (Committee) hearing, we will discuss this status report.

We did not perform procedures to substantiate any of the recommendations noted in OIT's public status report, as OIT reported that it had not implemented any of the recommendations it partially agreed to, as listed in the report.

Following the Committee's vote to go into executive session in accordance with Section 24-6-402(3)(a)(IV), C.R.S., we will distribute and discuss the status report for *Audit of Cybersecurity Resiliency at the Governor's Office of Information Technology – Confidential Report*.

The executive session will be held at approximately 11:30 a.m. during the December 9, 2024, Legislative Audit Committee hearing. The confidential material will be collected at the conclusion of the executive session.



**COLORADO**

**Governor's Office of  
Information Technology**

Serving People. Serving Colorado.

7/15/2024

Kerri L. Hunter, CPA, CFE  
State Auditor  
Colorado Office of the State Auditor  
1525 Sherman St., 7<sup>th</sup> Floor  
Denver, CO 80203

Dear Auditor Hunter:

In response to your request, we have prepared the attached status report on the implementation status of audit recommendations contained in the OIT Cybersecurity Resiliency Audit 2250P-IT. The report provides a brief explanation of the actions taken by the Governor's Office of Information Technology/Office of Information Security to implement each recommendation.

Much of the work to produce supporting artifacts continues and will be available per the prescribed dates.

Per OIT project tracking the percentage of complete recommendations is 23%. The Governor's Office of Information Technology/Office of Information Security continues to make the implementation of these audit recommendations its top priority and will achieve these remediations where appropriate by June 30, 2025. All but a handful of the 12 audit findings (77 recommendations) are in varying states of progress. Many were not capable of providing artifacts to qualify them as partially implemented at the time of this writing. OIT is tracking all of these efforts as projects and the current project progress value is 43%.

If you have any questions about this status report and the Governor's Office of Information Technology/Office of Information Security's efforts to implement the



audit recommendations, please contact Craig Hurter, Sr Director Information Security at 720-751-1266 or [craig.hurter@state.co.us](mailto:craig.hurter@state.co.us).

Sincerely,

DocuSigned by:  
*David Edinger*  
47928ED20CB34F0...

David Edinger  
Governor's Office of Information Technology/Office of Information Security



# Audit Recommendation Status Report

<b>Audit Name:</b>	Audit of Cybersecurity Resiliency – Public Report
<b>Audit Number:</b>	2250P-IT
<b>Agency:</b>	Governor’s Office of Information Technology
<b>Date of Status Report:</b>	July 2024

## Section I: Summary

Rec. Number	Response from Audit Report	Original Implementation Date	Current Implementation Status	Current Implementation Date
1A	<p>Recommendation 1 was included in the Fiscal Year 2023 Statewide Single Audit report, released in February 2024; Recommendation 1’s implementation status is, therefore, being conducted as part of the Fiscal Year 2024 Statewide Audit and will be included in that report. Therefore, Recommendation 1 will not be included in this status report.</p>			
1B				
1C				
1D				
1E				
1F				
1G				
1H				
2A	Partially Agree	June 2025	Not Implemented	December 2024
2B	Partially Agree	June 2025	Not Implemented	December 2024
2C	Partially Agree	December 2023	Not Implemented	December 2024
2D	Partially Agree	December 2023	Not Implemented	December 2024

## Section II: Narrative Detail

### Recommendation 2A

The Governor's Office of Information Technology should improve information security and training and awareness by:

- A. Establishing a formal training program for Business Owners that outlines and provides necessary direction on their security roles and responsibilities, especially those outlined in the Colorado Information Security Policies (CISPs).

<b>Current Implementation Status</b>	Not Implemented
--------------------------------------	-----------------

<b>Current Implementation Date</b>	December 2024
------------------------------------	---------------

<b>Status Update Narrative</b>	OIT is working on establishing a formal training program for Business Owners that outlines and provides necessary direction on their security roles and responsibilities, especially those outlined in the Colorado Information Security Policies (CISPs)
--------------------------------	---

### Recommendation 2B

The Governor's Office of Information Technology should improve information security and training and awareness by:

- B. Utilizing resources in more efficient ways to ensure IT directors receive formal training on their security roles and responsibilities, especially outlined in the CISPs.

<b>Current Implementation Status</b>	Not Implemented
--------------------------------------	-----------------

<b>Current Implementation Date</b>	December 2024
------------------------------------	---------------

<b>Status Update Narrative</b>	OIT is working to utilize resources in more efficient ways to ensure IT directors receive formal training on their security roles and responsibilities, especially those outlined in the CISPs.
--------------------------------	---

### Recommendation 2C

The Governor's Office of Information Technology should improve information security and training and awareness by:

- C. Enforcing sanctions for users who do not complete security awareness training in a timely manner.

<b>Current Implementation Status</b>	Not Implemented
--------------------------------------	-----------------

<b>Current Implementation Date</b>	December 2024
------------------------------------	---------------

<b>Status Update Narrative</b>	OIT is working on the following steps to enforce sanctions for users who do not complete security awareness training in a timely manner. 1. Develop a plan to enforce security awareness training and sanctions.
--------------------------------	---

	2. Communicate the enforcement plan with all state agencies (sharing and leveraging OIT policy and how to enforce).
--	---

<b>Recommendation 2D</b>	
The Governor’s Office of Information Technology should improve information security and training and awareness by:	
D. Enforcing sanctions for users who do not review and acknowledge the State’s Acceptable Use Policy at the start of employment and annually thereafter.	
<b>Current Implementation Status</b>	Not Implemented
<b>Current Implementation Date</b>	December 2024
<b>Status Update Narrative</b>	OIT is working on the following steps to enforce sanctions for users who do not review and acknowledge the State’s Acceptable Use Policy at the start of employment and annually thereafter: 1. Develop a plan to enforce acceptable use policy and sanctions. 2. Communicate the enforcement plan with all state agencies.