IT Performance Audit of Cybersecurity Resiliency at the Judicial Department

Judicial Department

IT Performance Audit of Cybersecurity Resiliency

Public Report

March 2025

Report Number 2453P-IT

Eide Bailly LLC

THE MISSION OF THE OFFICE OF THE STATE AUDITOR
IS TO IMPROVE GOVERNMENT
FOR THE PEOPLE OF COLORADO

LEGISLATIVE AUDIT COMMITTEE

Representative William Lindstedt Chair	Senator Lisa Frizell Vice Chair
Representative Max Brooks	Senator Rod Pelton
Representative Jarvis Caldwell	Senator Mike Weissman
Senator Dafna Michaelson Jenet	Representative Jenny Willford

OFFICE OF THE STATE AUDITOR

Kerri L. Hunter, CPA, CFE	State Auditor
Matt Devlin, CISA, CISM	Chief IT Auditor and Contract Monitor
Cindi Radke, CISA	IT Audit Manager
Eide Bailly LLP	Contractor

REPORT NUMBER 2453P-IT

EideBailly®

CPAs & BUSINESS ADVISORS

March 7, 2025

Members of the Legislative Audit Committee:

This report contains the results of the IT Performance Audit of Cybersecurity Resiliency at the Judicial Department. The audit was conducted pursuant to Section 2-3-103, C.R.S, which authorizes the State Auditor to conduct performance, financial, and information technology audits of all departments, institutions, and agencies of state government. The report presents our findings, conclusions, and recommendations, and the responses of the Judicial Department.

We conducted this performance audit in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

During our audit work, we identified certain matters that were considered sensitive to protecting state information technology assets. Accordingly, these matters are not included in this report but were reported to the Judicial Department's management in a separate confidential report dated March 7, 2025.

E. Anders Erickson
Principal, Risk Advisory Services
Eide Bailly, LLC

CONTENTS

REPORT HIGHLIGHTS

Audit of Cybersecurity Resiliency at the Judicial Department
IT Performance Evaluation, March 2025 – Report Number 2453P-IT

EVALUATION CONCERNS

Conducting audits that evaluate an organization's cybersecurity resilience can significantly enhance its ability to prevent, detect, and respond to cyber threats. By identifying vulnerabilities and addressing risks, these audits help reduce the likelihood and potential impact of security incidents. In turn, this strengthens the overall integrity of information systems and ensures the reliability of the data they manage, supporting both operational and strategic objectives.

The primary concern identified in this public report regarding the Judicial Department, as an independent agency within the state of Colorado, is its interpretation of the state statute C.R.S. 24-37.5-403, which defines public agency responsibilities. The issue revolves around the inconsistent application of statutory requirements related to being a public agency, particularly in terms of adherence to the state's information security policies (Colorado Information Security Policies, or CISPs, or Policies).

Additional concerns were identified in several key areas, including Risk Management; Policies and Procedures; Asset and Risk Identification; and Data and Information Protection, Detection, Response, and Recovery. Due to the sensitive nature of these issues, their details have been documented separately in a confidential report as Findings 2 through 6.

BACKGROUND

Judicial Department

- The Chief Justice has authority over all policies within the Judicial Department, which are issued in the form of Chief Justice Directives (CJDs).
- The Judicial Department has its own IT Division – Information Technology Services (ITS) – which is organizationally located within the Judicial Department's State Court Administrator's Office (SCAO).

KEY FACTS AND FINDINGS

- The Judicial Department and the State's Chief Information Security Officer within the Governor's Office of Information Technology provided different interpretations of Colorado statute Section 24-37.5-403, C.R.S., which defines public agency responsibilities related to adherence to the CISO-issued Colorado Information Security Policies, regarding whether Judicial is required to follow the Policies or not.
- The Judicial Department had not adopted or adhered to the CISPs.

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 2 through 6.

The box below provides a count of the total recommendations made as a result of 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 Judicial management agreed, partially agreed, or disagreed.

Recommendations Made

46

Responses

Agree: **46**

Partially Agree: **0**

Disagree: **0**

CHAPTER 1

OVERVIEW

Organizations conduct cybersecurity resiliency audits to assess the strength and effectiveness of their cybersecurity measures while identifying vulnerabilities and potential weaknesses in their systems. These audits help uncover security gaps, whether caused by outdated software, unsecured network devices, or inadequate security policies. By identifying these issues, organizations can take proactive steps to address vulnerabilities, strengthen their cybersecurity posture, and enhance their ability to prevent, detect, and respond to cyber threats.

Additionally, cybersecurity audits ensure compliance with relevant laws, regulations, and industry standards, while also verifying adherence to internal security policies and procedures. This process minimizes the risk and impact of security breaches, safeguarding both the organization's operations and its reputation. Ultimately, a cybersecurity resiliency audit serves as a critical tool for managing and mitigating the risks associated with an increasingly complex cyber threat landscape.

Judicial Department

The Colorado Judicial Branch (Judicial Branch), one of three branches of state government, is responsible for interpreting and applying the State's laws. It includes the Colorado Supreme Court, Court of Appeals, 22 judicial districts[1] with district and county courts, and specialized courts such as water, probate, and problem-solving courts. Each of the State's Judicial Districts is led by a Chief Judge, a Court Executive, and a Chief Probation Officer. The Court Executive, a professional working under the direction of the Chief Judge, manages the non-judicial operations of the court. The Judicial Branch provides judicial and probation services across the state and is supported by the State Court Administrator's Office, which oversees administration, budgeting, and policy implementation. Operating independently of the executive and legislative branches, the Judicial Branch ensures an impartial system for resolving disputes, protecting rights, and upholding the rule of law.

Information Technology Services (ITS)

The Information Technology Services (ITS) Division of the Judicial Branch resides within the State Court Administrator's Office and supports the technology needs of the state's judicial system. This includes providing IT services to the Supreme Court, Court of Appeals, all 22 judicial and probation districts[1] across Colorado, and the State Court Administrator's Office. ITS also manages integrations with other government agencies and ensures digital access to Judicial Branch services for the public. Notably, the ITS Division does not provide IT support for independent agencies within the Judicial Branch which include the Office of the State Public Defender (OSPD), Office of Alternate Defense Counsel (OADC), Office of the Child's Representative (OCR), Office of the Respondent Parents' Counsel (ORPC), Office of Administrative Services for Independent Agencies (ASIA), Office of the Child Protection Ombudsman (OCPO), Independent Ethics Commission (IEC), Office of Public Guardianship (OPG), Commission on Judicial Discipline, and Statewide Behavioral Health Court Liaison Office (Bridges). Instead, IT support for these independent agencies is provided internally by their agency or by another IT service provider. As

[1] At the time of our audit, there were 22 judicial districts. An additional judicial district was added on January 7, 2025.

this audit focused on the ITS Division of the Judicial Branch, these independent agencies were not within the scope of this audit.

The ITS leadership team is composed of a Chief Information Officer (CIO), three deputy directors, and nine managers, each overseeing specific departments within ITS. These departments include Information Security, Application Development, Infrastructure, Networking, Technical Support, Audio Visual, Business Operations, Information Management, and the Project Management Office.

Audit Objectives, Scope, and Methodology

We conducted this performance audit pursuant to Section 2-3-103, C.R.S., which authorizes the State Auditor to conduct audits of all departments, institutions, and agencies of the state government. Our audit period for this audit was July 2023 through June 2024. The audit work was performed from June 2024 through October 2024, and we appreciate the cooperation and assistance provided by the Judicial Department's management and staff throughout the process.

This performance audit was conducted in accordance with generally accepted government auditing standards. These standards require audits to be planned and executed to obtain sufficient, appropriate evidence that provides a reasonable basis for the findings and conclusions related to the audit objectives. We believe the evidence obtained meets these requirements and supports our findings and conclusions.

The key objectives of the audit include the following: (1) determine whether ITS had adequate cybersecurity practices in place to govern, identify, protect, detect, respond to, and recover from cybersecurity events that could impact the Judicial Department's critical infrastructure, IT systems, data, and business operations; (2) identify areas for improvement, if any, that could enhance the security and resilience of Judicial's critical IT systems and infrastructure; and (3) determine whether the Judicial Department is complying with all applicable state statutes.

To accomplish our audit objectives, we performed numerous auditing activities and utilized various sampling techniques. These activities and sampling techniques are outlined in each individual finding within the report.

As required by auditing standards, we planned our audit work to assess the effectiveness of those internal controls that were significant to our audit objectives. Details about the audit work supporting our findings and conclusions, including any deficiencies in internal control that were significant to our audit objectives, are described in the remainder of this report. To address concerns regarding the state's cybersecurity posture, specific details about deficiencies identified in Risk Management; Policies and Procedures; Asset and Risk Identification; and Data and Information Protection, Detection, Response, and Recovery are documented in a separate, confidential report. Findings 2 through 6, which address these areas, are included in that confidential report.

The scope and methodology of this cybersecurity resiliency audit utilized the universally recognized standards of the National Institute of Standards and Technology (NIST) Cybersecurity Framework (CSF) 2.0, alongside NIST Special Publication 800-53 Security and Privacy Controls for Information Systems and Organizations Rev. 5, to assess the effectiveness of Judicial's cybersecurity practices. These standards and frameworks are widely applicable across all types of organizations, ensuring comprehensive coverage of cybersecurity risks and controls. The audit focused on Judicial's ability to meet security practices outlined in the six core functions of the NIST CSF: Govern, Identify, Protect, Detect, Respond, and Recover.

- **Govern** – The organization's ability to establish, monitor, and maintain a cybersecurity risk management strategy, expectations, and policies.
- **Identify** – The organization's ability to recognize and manage cybersecurity risks and vulnerabilities.
- **Protect** – The implementation of controls designed to safeguard against cyber threats.
- **Detect** – The organization's ability to identify and detect cybersecurity incidents in a timely manner.
- **Respond** – The organization's ability to respond effectively to cybersecurity incidents, minimizing their impact.
- **Recover** – The organization's ability to restore normal business operations following a cybersecurity incident.

A draft of this report was reviewed by Judicial. Obtaining the views of responsible officials is an important part of ensuring that the report is accurate, complete, and objective. We, along with the Colorado Office of the State Auditor (OSA), were responsible for determining whether and how to revise the report, if appropriate, based on Judicial's comments. The written responses to the recommendations and the related implementation dates were the sole responsibility of Judicial. However, in accordance with auditing standards, we have included Auditor's Addendums to responses that are inconsistent or in conflict with the findings or conclusions or do not adequately address the recommendations.

CHAPTER 2
PUBLIC FINDINGS AND INFORMATION

Finding 1: Statutory Requirements

Colorado Revised Statute (C.R.S.) Title 24, Article 37.5 establishes the Governor's Office of Information Technology (OIT) and, among other things, defines the duties and responsibilities of the state's Chief Information Security Officer (CISO). These CISO responsibilities related to information security policies, standards, and guidelines include the following:

- Developing and updating information security policies, standards, and guidelines for *public agencies*.
- Promulgating information security policies, standards, and guidelines.
- Ensuring the incorporation of and compliance with information security policies, standards, and guidelines in the information security plans developed by *public agencies*.
- Directing information security audits and assessments in *public agencies* to ensure program compliance and adjustments.

C.R.S.24-37.5-102(26) defines a *public agency* as, "…every state office, whether executive or ***judicial*****,** [emphasis added] and all of its respective offices, departments, divisions, commissions, boards, bureaus, and institutions."

In response to the requirements of C.R.S. 24-37.5-403(2)(a), the CISO has released a series of policies referred to as the Colorado Information Security Policies (CISPs). The "Organizations Affected" section of each CISP states, "This policy applies to any and every ***public agency*** [emphasis added] as defined in C.R.S. 24-37.5-102(26)." As of the time of our assessment, Judicial had not adhered to the CISPs or adopted them as the basis for their information security policies, standards, or guidelines.

What was the purpose of our audit work and what audit work was performed?

The purpose of the audit work was to determine whether the Colorado Judicial Department is required to adhere to CISPs issued by OIT CISO.

To conduct our audit and support our conclusions, we interviewed Colorado Judicial Department's (Judicial) leadership as well as the State's CISO. In addition, at our request, the Colorado Office of the State Auditor sought input from Colorado General Assembly's Office of Legislative Legal Services regarding whether the Judicial Department is required to adhere to the information security policies and standards developed by the state's Chief Information Security Officer (CISO) pursuant to section 24-37.5-403 (2), C.R.S.

What problems did the audit work identify and how were the results measured?

We identified the following problem with the Colorado Judicial Department's interpretation of certain IT-related statutory requirements:

The Colorado Judicial Department's interpretation of its responsibility to adhere to the CISPs developed by the State's CISO differs from that of the State's CISO.

When we presented Judicial management and the State CISO with the statutory excerpts outlined in the introductory paragraphs of this finding and asked their interpretation of Judicial's responsibility to adhere to the CISPs, we obtained the following responses:

From Judicial Leadership:

"The Judicial Department looks to those policies for guidance, but the CISPs are not binding on Judicial. The Chief Justice, as the executive head of Judicial, has sole authority to administer Judicial's Information Technology Services (ITS) system."

From the State's Chief Information Security Officer:

"It is my interpretation that Judicial adheres to the CISPs."

Because of the apparent difference of opinions between Judicial and OIT regarding whether Judicial is required to adhere to State CISO-issued information security policies and standards, we also reached out to the General Assembly's Office of Legislative Legal Services (OLLS). OLLS staff indicated that, because Judicial is included in the CISO statutes in the definition of "public agency," the provisions of the information security statute, including the requirement to adhere to information security policies and standards developed by the CISO (pursuant to Section 24-37.5-403(2), C.R.S.) currently apply to Judicial.

In its response, OLLS Staff also observed that statute creates a separate term, "state agency" that refers to, "…all of the departments, divisions, commissions, boards, bureaus, and institutions in the executive branch of the state government," but excludes (among other bodies) the judicial department. Based on the creation of these two definitions – *public agency* and *state agency* – OLLS Staff noted that, "the General Assembly intended to use the definition of "public agency" rather than "state agency" to apply to part 4, and therefore intended to include the Judicial Department in the requirements of the information security statute."

We also noted that Standards for Internal Control in the Federal Government (Green Book) Principle 6.05 states that management should consider external requirements and internal expectations when defining objectives to enable the design of internal control. Legislators, regulators, and standard-setting bodies set external requirements by establishing the laws, regulations, and standards with which the entity is required to comply. Management should identify, understand, and incorporate these requirements into the entity's objectives.

Why did the problems occur?

Based upon our test results and discussions with Judicial, this problem occurred because Judicial had not established a consistent interpretation of Title 24, Article 37.5 and had not vetted that interpretation with all impacted parties. As an example of this inconsistent interpretation, while Judicial ensured

compliance with C.R.S. 24-37.5-404 by submitting an annual information security plan to the State's CISO for approval, they did not adhere to C.R.S. 24-37.5-403 by adopting the information security policies, standards, and guidelines for public agencies established by the State's CISO.

Why do these problems matter?

In establishing the requirements within Title 24, Article 37.5 and explicitly including Judicial in the definition of a public agency, the General Assembly set its expectation that the policies for information security at Judicial need to align with those established by the State's CISO. To help ensure the security of the State's systems and information as a whole, without apparent gaps, it is important for Judicial to adopt the statutorily required framework for its policies and overall approach to information security. By not adopting the CISPs, Judicial failed to establish the level of information security maturity intended by the General Assembly and necessary to manage and mitigate the information security risks it faces.

Recommendation No. 1:

The Colorado Judicial Department should resolve conflicting interpretations of its statutory requirements by utilizing the Colorado Information Security Policies (CISPs) developed by the Governor's Office of Information Technology's (OIT) Chief Information Security Officer (CISO) as the foundation upon which Judicial's information security policies and procedures are built. Alternatively, the Colorado Judicial Department should seek statutory change to remove Judicial from the definition of "public agency," as currently defined in C.R.S 24-37.5-102(26).

Agency Responses:

Recommendation No. 1:

Agree. Implementation Date: September 2025.
The Judicial Department is concerned about any statutory provisions or actions by CISO or OIT that would interfere with the Judicial Department's essential function as a separate and co-equal branch of government.

Therefore, the Judicial Department agrees to consult with the Governor's Office of Information Technology (OIT) and utilize OIT's CISP as the foundation upon which to develop the Judicial Department's information security policies, ensuring alignment and separation across separate branches of government.

Further, Judicial Department agrees that, as a "public agency" for purposes of the Office of Information Technology (OIT), it is required to develop an information security plan "utilizing the information security policies, standards, and guidelines developed" by the Chief Information Security Officer (CISO). § 24-37.5-404(1). The Judicial Department will continue to submit an annual security plan in compliance with section 24-37.5-404.

Glossary

Asset Management

The process of identifying, tracking, and managing an organization's assets to optimize their use and reduce risks.

Contingency Planning

Preparing strategies and procedures to maintain or restore operations during and after unexpected disruptions or emergencies.

Cybersecurity

The practice of protecting or defending the organization's systems, networks, programs, data, etc. from cyberattacks, whether criminal or unintentional unauthorized access.

Cybersecurity Posture

The overall security status of an organization's IT systems, processes, and controls, reflecting its ability to detect, prevent, and respond to cyber threats.

Cybersecurity Practices

The set of strategies, protocols, and measures designed to protect computer systems, networks, and data from unauthorized access, attacks, and damage.

Incident Response

A structured approach to identifying, managing, and mitigating the impact of security incidents or breaches.

Identification and Authentication

The process of verifying the identity of users, systems, or devices and allowing access only to authorized entities through the use of credentials and authentication mechanisms.

Information Security

The protection of information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide confidentiality, integrity, and availability.

Information Security Policy

A formal document that defines required security safeguards for all aspects of information systems, information technology, IT assets and data protection.

Information System

A combination of hardware, software, and processes designed to collect, process, store, and share information.

IT Support

Services provided to assist users with technical issues, system maintenance, and IT infrastructure management.

Logging and Monitoring

The practice of recording system activities and continuously observing them to detect anomalies, breaches, or performance issues.

National Institute of Standards and Technology (NIST)

NIST is located within the Federal Department of Commerce and develops standards that are applicable to the federal government and can be adopted by other organizations.

National Institute of Standards and Technology (NIST) Cybersecurity Framework (CSF) 2.0

A set of guidelines and best practices from the National Institute of Standards and Technology (NIST) for managing and reducing cybersecurity risks, updated in its second version.

National Institute of Standards and Technology (NIST) Special Publication 800-53 Rev. 5

A comprehensive catalog of security and privacy controls for federal information systems and organizations, designed to manage risks effectively.

Patch Management

The process of acquiring, testing, and deploying updates to software or firmware to fix vulnerabilities and improve functionality.

Physical Access Controls

Measures designed to prevent unauthorized access to physical locations, devices, or assets, such as locks, badges, or biometric systems.

Public Agency

Every state office, whether executive or judicial, and all of its respective offices, departments, divisions, commissions, boards, bureaus, and institutions. “Public agency” does not include institutions of higher education or the general assembly. (C.R.S.24-37.5-102(26))

Risk Management

The process of identifying, assessing, and mitigating risks to minimize their impact on an organization’s objectives.

Security Incident

An event that compromises the confidentiality, integrity, or availability of information or systems, requiring investigation and response.

Security Planning

The process of defining security policies, objectives, and strategies to protect an organization’s assets and operations.

State Agency

All of the departments, divisions, commissions, boards, bureaus, and institutions in the executive branch of the state government. “State agency” does not include the legislative or judicial department, the department of education, the department of law, the department of

state, the department of the treasury, or state-supported institutions of higher education. (C.R.S.24-37.5-102(28))

User Account Management

The process of creating, maintaining, and controlling user accounts and their access to systems and data.

Vulnerability

A weakness in a system, process, or application that could be exploited to compromise its security.