Second Regular Session
Seventy-fifth General Assembly
STATE OF COLORADO

DRAFT

REDRAFT
4/22/26
Double underlining denotes changes from prior draft

LLS NO. 26-0979.02 Nicole Myers x4326 **COMMITTEE BILL**

Joint Technology Committee

BILL TOPIC: Enhance Security of Office of Info Tech

A BILL FOR AN ACT

CONCERNING MEASURES TO ENHANCE THE OFFICE OF INFORMATION TECHNOLOGY'S SECURITY PROCEDURES.

Bill Summary

(Note: This summary applies to this bill as introduced and does not reflect any amendments that may be subsequently adopted. If this bill passes third reading in the house of introduction, a bill summary that applies to the reengrossed version of this bill will be available at http://leg.colorado.gov/.)

Joint Technology Committee. The bill allows the joint technology committee (JTC), _____ within 90 days after the day that the chief information security officer of the office of information technology (security officer) files a written information technology compliance report (compliance report) with the JTC as required by the bill, to vote to request that the state auditor conduct an information technology security audit (IT

security audit) of the office of information technology (OIT) if the compliance report represents that OIT fully resolved one or more audit recommendations or if a material discrepancy exists between a representation in the compliance report and a previous audit finding.

If the JTC votes to request an IT security audit, the bill requires:

- The state auditor to conduct the IT security audit;
- The state auditor to submit the IT security audit report to the JTC, the legislative audit committee, the joint budget committee, and the governor; and
- OIT to reimburse the state auditor for the auditor's costs incurred in completing the IT security audit.

The bill requires OIT to establish, maintain, keep, and quarterly update a publicly available list of all active information technology vendor contracts, including contracts entered into by state agencies and private sector providers of information technology resources and contracts related to the procurement of information technology resources for state agencies.

The bill specifies that OIT shall not publish or implement a technical information technology standard, and that the standard is void, unless the standard:

- Was publicly posted on OIT's website _____; and
- Received approval from the security officer if the standard relates to security, access controls, or the handling of data.

The bill prohibits the chief information officer from delegating a duty, responsibility, or power of the security officer and requires the security officer to submit to the JTC, on or before November 1 of each year, a written compliance report that includes the following information:

- OIT's current compliance status with applicable security standards;
- All open audit recommendations regarding OIT made by the state auditor and the date on which each recommendation was made; and
- A timeline for remediation for each open audit recommendation made by the state auditor.

Be it enacted by the General Assembly of the State of Colorado:

SECTION 1. In Colorado Revised Statutes, 2-3-1704, **add** (13), (14), and (15) _____ as follows:

2-3-1704. Powers and duties of the joint technology committee.

REDRAFT
4/22/26
Double underlining denotes changes from prior draft

(13) THE COMMITTEE MAY CALL THE CHIEF INFORMATION SECURITY OFFICER TO TESTIFY BEFORE THE COMMITTEE REGARDING THE WRITTEN INFORMATION TECHNOLOGY SECURITY COMPLIANCE REPORT THAT THE CHIEF INFORMATION SECURITY OFFICER IS REQUIRED TO SUBMIT TO THE COMMITTEE PURSUANT TO SECTION 24-37.5-403 (2)(j).

(14) WITHIN NINETY DAYS AFTER THE DAY THAT THE CHIEF INFORMATION SECURITY OFFICER OF THE OFFICE OF INFORMATION TECHNOLOGY FILES A WRITTEN INFORMATION TECHNOLOGY SECURITY COMPLIANCE REPORT AS REQUIRED BY SECTION 24-37.5-403 (2)(j), THE COMMITTEE MAY VOTE TO FORMALLY REQUEST THAT THE STATE AUDITOR, PURSUANT TO THE STATE AUDITOR'S AUTHORITY RELATED TO INFORMATION TECHNOLOGY SYSTEMS AS DESCRIBED IN SECTION 2-3-103 (1.5), CONDUCT AN INFORMATION TECHNOLOGY SECURITY AUDIT OF THE OFFICE OF INFORMATION TECHNOLOGY AND ALL OF THE INFORMATION TECHNOLOGY CONTRACTS TO WHICH THE OFFICE OF INFORMATION TECHNOLOGY IS AN ACTIVE PARTY IF:

(a) THE WRITTEN INFORMATION TECHNOLOGY SECURITY COMPLIANCE REPORT REQUIRED BY SECTION 24-37.5-403 (2)(j) REPRESENTS THAT THE OFFICE OF INFORMATION TECHNOLOGY HAS FULLY REMEDIATED AND RESOLVED ONE OR MORE RECOMMENDATIONS MADE BY THE STATE AUDITOR IN A PREVIOUS AUDIT; OR

(b) A MATERIAL DISCREPANCY EXISTS BETWEEN A REPRESENTATION MADE IN THE WRITTEN INFORMATION TECHNOLOGY SECURITY COMPLIANCE REPORT REQUIRED BY SECTION 24-37.5-403 (2)(j) AND A FINDING MADE IN:

(I) A PREVIOUS AUDIT OF THE STATE AUDITOR;

REDRAFT
4/22/26
Double underlining denotes changes from prior draft

(II) A PRIOR RESPONSE TO A REQUEST FOR INFORMATION FROM THE COMMITTEE; OR

(III) OTHER DOCUMENTED EVIDENCE BEFORE THE COMMITTEE.

(15) IF A MAJORITY OF THE COMMITTEE VOTES TO REQUEST AN INFORMATION TECHNOLOGY SECURITY AUDIT PURSUANT TO SUBSECTION (14) _____ OF THIS SECTION, THE STATE AUDITOR SHALL CONDUCT THE INFORMATION TECHNOLOGY SECURITY AUDIT AND MAY CONTRACT WITH A QUALIFIED THIRD-PARTY INFORMATION TECHNOLOGY SECURITY FIRM TO CONDUCT THE AUDIT. THE STATE AUDITOR SHALL, WITHIN ONE HUNDRED EIGHTY DAYS OF THE AFFIRMATIVE VOTE OF A MAJORITY OF THE COMMITTEE, SUBMIT THE INFORMATION TECHNOLOGY SECURITY AUDIT REPORT TO THE COMMITTEE, THE LEGISLATIVE AUDIT COMMITTEE, THE JOINT BUDGET COMMITTEE, AND THE GOVERNOR. PURSUANT TO SECTION 2-3-110, THE OFFICE SHALL REIMBURSE THE STATE AUDITOR FOR AN AUDIT CONDUCTED PURSUANT TO SUBSECTION (14) ____ OF THIS SECTION. THE REIMBURSEMENT MUST BE PAID FROM THE TECHNOLOGY RISK PREVENTION AND RESPONSE FUND CREATED IN SECTION 24-37.5-120.

SECTION 2. In Colorado Revised Statutes, 24-37.5-105, **amend** (3)(c) and (3)(d); and **add** (3)(e), (4.5), and (4.7) as follows:

24-37.5-105. Office - roles - responsibilities - state search interface - rules - legislative declaration - definitions.

(3) The office shall:

(c) Assist the joint technology committee as necessary to facilitate the committee's oversight of the office; ~~and~~

(d) Establish, maintain, and keep an inventory of information technology owned by or held in trust for every state agency; AND

(e) ESTABLISH, MAINTAIN, KEEP, AND QUARTERLY UPDATE A

REDRAFT
4/22/26
Double underlining denotes changes from prior draft

PUBLICLY AVAILABLE LIST OF ALL ACTIVE INFORMATION TECHNOLOGY VENDOR CONTRACTS, INCLUDING CONTRACTS ENTERED INTO BY STATE AGENCIES AND PRIVATE SECTOR PROVIDERS OF INFORMATION TECHNOLOGY RESOURCES AND CONTRACTS RELATED TO THE PROCUREMENT OF INFORMATION TECHNOLOGY RESOURCES FOR STATE AGENCIES AS DESCRIBED IN SUBSECTION (6) OF THIS SECTION. FOR EACH INFORMATION TECHNOLOGY VENDOR CONTRACT, THE LIST MUST INCLUDE:

(I) THE NAME OF THE VENDOR;

(II) THE VALUE OF THE CONTRACT;

(III) THE DATE ON WHICH THE CONTRACT EXPIRES; AND

(IV) THE SECURITY CLASSIFICATION TIER OF THE CONTRACT.

(4.5) THE OFFICE SHALL SUBMIT A ONE-TIME INFORMATION TECHNOLOGY BUDGET REQUEST TO THE JOINT TECHNOLOGY COMMITTEE FOR THE COST OF BUILDING AND IMPLEMENTING THE LIST OF ACTIVE INFORMATION TECHNOLOGY VENDOR CONTRACTS REQUIRED BY SUBSECTION (3)(e) OF THIS SECTION. IF, AFTER THE BUDGET REQUEST IS APPROVED, THE OFFICE DETERMINES THAT MORE MONEY IS NEEDED TO IMPLEMENT AND MAINTAIN THE LIST, THE OFFICE MAY REQUEST THAT THE GENERAL ASSEMBLY ALLOCATE ADDITIONAL MONEY FROM THE TECHNOLOGY RISK PREVENTION AND RESPONSE FUND CREATED IN SECTION 24-37.5-120.

(4.7) THE OFFICE SHALL NOT PUBLISH OR IMPLEMENT A TECHNICAL INFORMATION TECHNOLOGY STANDARD THAT IS ESTABLISHED PURSUANT TO SUBSECTION (4) OF THIS SECTION, AND THE STANDARD IS VOID, UNLESS:

(a) THE OFFICE HAS PUBLICLY POSTED THE STANDARD ON THE OFFICE'S WEBSITE ____; AND

(b) THE CHIEF INFORMATION SECURITY OFFICER HAS APPROVED THE STANDARD, IF THE STANDARD RELATES TO SECURITY, ACCESS CONTROLS, OR THE HANDLING OF DATA.

SECTION 3. In Colorado Revised Statutes, 24-37.5-105.4, **amend** (1) introductory portion as follows:

24-37.5-105.4. Delegation of authority.

(1) The chief information officer may delegate an information technology function of the office to another state agency by agreement or other means authorized by law, EXCEPT THAT THE CHIEF INFORMATION OFFICER SHALL NOT DELEGATE A DUTY, RESPONSIBILITY, OR POWER OF THE CHIEF INFORMATION SECURITY OFFICER. The chief information officer may delegate an information technology function of the office if in the judgment of the director of the state agency and the chief information officer:

SECTION 4. In Colorado Revised Statutes, 24-37.5-403, **amend** (1), (2)(h), and (2)(i); and **add** (2)(j), and (4) _____ as follows:

24-37.5-403. Chief information security officer - duties and responsibilities.

(1) The chief information officer shall appoint a chief information security officer who shall serve at the pleasure of the chief information officer. The security officer shall report to and be under the supervision of the chief information officer. The security officer shall exhibit a background and expertise in security and risk management for communications and information resources. In the event the security officer is unavailable to perform the duties and responsibilities under this part 4, all powers and authority granted to the security officer ~~may~~ MUST be exercised by the chief information officer.

(2) The chief information security officer shall:

(h) In coordination and consultation with the office of state planning and budgeting and the chief information officer, review public agency budget requests related to information security systems and approve such budget requests for state agencies other than the legislative department; ~~and~~

(i) Coordinate with the Colorado commission on higher education ~~for purposes of reviewing and commenting~~ TO REVIEW AND COMMENT on information security plans adopted by institutions of higher education that are submitted pursuant to section 24-37.5-404.5 (3); AND

(j) SUBMIT TO THE JOINT TECHNOLOGY COMMITTEE, ON OR BEFORE NOVEMBER 1, 2026, AND ON OR BEFORE NOVEMBER 1 OF EACH YEAR THEREAFTER, A WRITTEN INFORMATION TECHNOLOGY SECURITY COMPLIANCE REPORT THAT INCLUDES THE FOLLOWING INFORMATION:

(I) THE OFFICE'S CURRENT COMPLIANCE STATUS WITH APPLICABLE SECURITY STANDARDS;

(II) ALL OPEN AUDIT RECOMMENDATIONS MADE BY THE OFFICE OF THE STATE AUDITOR AND THE DATE ON WHICH EACH RECOMMENDATION WAS MADE; AND

(III) A TIMELINE FOR REMEDIATION FOR EACH OPEN RECOMMENDATION MADE BY THE OFFICE OF THE STATE AUDITOR.

(4) THE CHIEF INFORMATION SECURITY OFFICER, OR THE CHIEF INFORMATION OFFICER IF THE SECURITY OFFICER IS UNAVAILABLE, SHALL PERFORM THE DUTIES AND UPHOLD THE RESPONSIBILITIES ASSIGNED TO THE CHIEF INFORMATION SECURITY OFFICER PURSUANT TO THIS PART 4. SUCH DUTIES AND RESPONSIBILITIES MUST NOT BE OTHERWISE DELEGATED.

REDRAFT
4/22/26
Double underlining denotes changes from prior draft

SECTION 5. Safety clause. The general assembly finds, determines, and declares that this act is necessary for the immediate preservation of the public peace, health, or safety or for appropriations for the support and maintenance of the departments of the state and state institutions.