**Second Regular Session**
**Seventy-fifth General Assembly**
**STATE OF COLORADO**

**INTRODUCED**

LLS NO. 26-0979.02 Nicole Myers x4326 **SENATE BILL 26-185**

**SENATE SPONSORSHIP**

**Marchman and Baisley,**

**HOUSE SPONSORSHIP**

**Titone and Keltie,** Paschal

**Senate Committees**
Business, Labor, & Technology

**House Committees**

## 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 legislative audit committee direct the state auditor to conduct a

special information technology security audit (IT security audit) of the office of information technology (OIT) if the compliance report indicates that one or more audit recommendations made by the state auditor is unresolved 2 or more years past the implementation date for the audit recommendation 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 and if the legislative audit committee votes to direct the audit, the bill requires:

- The state auditor to conduct the IT security audit;
- The state auditor to obtain input from OIT when the state auditor determines the scope and boundaries of the audit;
- The state auditor to submit the IT security audit report to the legislative audit committee, the JTC, 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, update, and make available to state agency information technology leadership and the members of the JTC, a list of all active information technology vendor contracts for state agencies.

The bill specifies that, except in the case of an information technology security emergency, OIT shall not publish or implement a technical information technology standard, and that the standard is void, unless the standard:

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

The bill requires OIT to ensure that, if an information technology contract provides ongoing service and delivery to Coloradans, that the contract maintains current architecture diagrams that are updated at least annually.

The bill prohibits the chief information officer from delegating a duty, responsibility, or power of the security officer.

The bill requires the security officer to submit 2 annual reports to the JTC. The first report is a written compliance report that includes 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 and a mitigation plan or compensation controls for each open audit recommendation made by the state auditor.

The second report is a written statewide information technology security risk report (security risk report) that assesses the overall security risk posture of state agency information technology systems. To support the preparation of the security risk report, the security officer may conduct evaluations of state agency information technology systems,

including penetration testing, vulnerability scanning, configuration evaluations, and vendor and system reviews. Each state agency shall provide to the security officer, upon request, the access and information necessary to conduct evaluations of state agency technology systems, including system access, product information, and architecture information.

The bill requires the security officer, or the chief information officer if the security officer is unavailable, to perform the duties and uphold the responsibilities assigned to the security officer pursuant to law.

---

*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.**

(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 LEGISLATIVE AUDIT COMMITTEE, PURSUANT TO SECTION 2-3-108, VOTE TO DIRECT A SPECIAL INFORMATION TECHNOLOGY SECURITY AUDIT OF THE OFFICE IN ACCORDANCE WITH THE STATE AUDITOR'S AUTHORITY RELATED TO INFORMATION TECHNOLOGY SYSTEMS AS DESCRIBED IN SECTION 2-3-103 (1.5), IF:

(a) THE WRITTEN INFORMATION TECHNOLOGY SECURITY

COMPLIANCE REPORT REQUIRED BY SECTION 24-37.5-403 (2)(j) INDICATES THAT ONE OR MORE AUDIT RECOMMENDATIONS MADE BY THE STATE AUDITOR IS UNRESOLVED TWO OR MORE YEARS PAST THE IMPLEMENTATION DATE FOR THE AUDIT RECOMMENDATION TO WHICH THE OFFICE COMMITTED IN A PRIOR COMPLIANCE REPORT; 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 A PREVIOUS AUDIT BY THE STATE AUDITOR.

(15) (a) IF A MAJORITY OF THE COMMITTEE VOTES TO REQUEST THAT THE LEGISLATIVE AUDIT COMMITTEE DIRECT A SPECIAL INFORMATION TECHNOLOGY SECURITY AUDIT PURSUANT TO SUBSECTION (14) OF THIS SECTION AND IF A MAJORITY OF THE LEGISLATIVE AUDIT COMMITTEE VOTES TO APPROVE AN AUDIT PURSUANT TO SECTION 2-3-108, 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 OBTAIN INPUT FROM THE OFFICE OF INFORMATION TECHNOLOGY WHEN THE STATE AUDITOR DETERMINES THE SCOPE AND BOUNDARIES OF THE AUDIT, TAKING INTO CONSIDERATION THE RESOURCES AVAILABLE TO THE OFFICE TO REIMBURSE THE AUDITOR FOR THE COST OF THE AUDIT PURSUANT TO SUBSECTION (15)(b) OF THIS SECTION.

(b) THE STATE AUDITOR SHALL, WITHIN TWELVE MONTHS OF THE AFFIRMATIVE VOTE OF A MAJORITY OF THE COMMITTEE, PRODUCE AN INFORMATION TECHNOLOGY SECURITY AUDIT REPORT AND SUBMIT THE AUDIT REPORT TO THE LEGISLATIVE AUDIT COMMITTEE, AFTER WHICH THE STATE AUDITOR SHALL SUBMIT THE REPORT TO THE 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 MAY 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), (3)(d), (6)(c), and (6)(d); and **add** (3)(e), (4.5), and (6)(e) 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) (I) ESTABLISH, MAINTAIN, KEEP, QUARTERLY UPDATE, AND MAKE AVAILABLE TO STATE AGENCY INFORMATION TECHNOLOGY LEADERSHIP AND THE MEMBERS OF THE JOINT TECHNOLOGY COMMITTEE, A LIST OF ALL ACTIVE INFORMATION TECHNOLOGY VENDOR CONTRACTS FOR STATE AGENCIES AS DESCRIBED IN SUBSECTION (6) OF THIS SECTION. FOR EACH INFORMATION TECHNOLOGY VENDOR CONTRACT, THE LIST MUST INCLUDE:

(A) THE NAME OF THE VENDOR;

(B) THE VALUE OF THE CONTRACT;

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

(D) THE DATA CLASSIFICATION - BUSINESS CRITICALITY TIER OF THE CONTRACT.

(II) IF A STATE AGENCY INITIATES SOLICITATIONS AND CONTRACTS FOR INFORMATION TECHNOLOGY RESOURCES WITH PRIOR APPROVAL OF THE PROCUREMENT OFFICIAL FOR THE OFFICE PURSUANT TO SUBSECTION (6) OF THIS SECTION, THE STATE AGENCY SHALL PROVIDE TO THE OFFICE THE INFORMATION SPECIFIED IN SUBSECTION (3)(e)(I) OF THIS SECTION FOR EACH INFORMATION TECHNOLOGY VENDOR CONTRACT, AND THE OFFICE SHALL INCLUDE THE INFORMATION IN THE LIST REQUIRED BY THIS SUBSECTION (3)(e).

(III) 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 REQUIRED BY THIS SUBSECTION (3)(e). 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.

(4.5) **Technical information technology standards.** (a) EXCEPT AS OTHERWISE PROVIDED IN SUBSECTION (4.5)(b) OF THIS SECTION, 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:

(I) THE OFFICE HAS PUBLICLY POSTED THE STANDARD; AND

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

(b) THE PROVISIONS OF SUBSECTION (4.5)(a) OF THIS SECTION DO NOT APPLY WHEN THE CHIEF INFORMATION SECURITY OFFICER DETERMINES

IN WRITING THAT AN INFORMATION TECHNOLOGY SECURITY EMERGENCY EXISTS. FOR PURPOSES OF THIS SUBSECTION (4.5), AN INFORMATION TECHNOLOGY SECURITY EMERGENCY MEANS A SITUATION IN WHICH AN IMMINENT OR ACTIVE THREAT TO STATE INFORMATION TECHNOLOGY SYSTEMS REQUIRES THE IMMEDIATE IMPLEMENTATION OF A SECURITY STANDARD TO PREVENT OR MITIGATE SIGNIFICANT HARM TO STATE DATA, SYSTEMS, OR OPERATIONS.

(c) IF THE OFFICE IMPLEMENTS A SECURITY STANDARD IN RESPONSE TO AN INFORMATION TECHNOLOGY SECURITY EMERGENCY PURSUANT TO SUBSECTION (4.5)(b) OF THIS SECTION, THE OFFICE SHALL POST THE STANDARD ON THE OFFICE'S WEBSITE WITHIN SEVENTY-TWO HOURS OF THE IMPLEMENTATION OF THE SECURITY STANDARD. A SECURITY STANDARD IMPLEMENTED PURSUANT TO SUBSECTION (4.5)(b) OF THIS SECTION EXPIRES NINETY DAYS AFTER IMPLEMENTATION UNLESS, PRIOR TO EXPIRATION, THE OFFICE COMPLIES WITH THE REQUIREMENTS OF SUBSECTION (4.5)(a) OF THIS SECTION.

(6) **Technology purchasing.** The office shall initiate the procurement of information technology resources for state agencies and enter into agreements or contracts on behalf of a state agency, multiple agencies, or the office, or be a party to procurement contracts that are initiated by state agencies. A state agency may initiate solicitations and contracts for information technology resources only with prior approval of the procurement official for the office, and must include provisions allowing the office to enforce technology and security standards or conduct due diligence or audits of the contractors. If the state agency does not receive written approval or disapproval from the procurement official for the office within thirty business days after submitting the procurement

request to the office for review, the state agency may assume that it has received the prior approval of the office, as required by this subsection (6), and is authorized to initiate the procurement or solicitation process. In connection with the procurement of information technology resources, the office shall:

(c) Oversee information technology vendors on behalf of the state and state agencies except when delegated to a state agency pursuant to section 24-37.5-105.4; ~~and~~

(d) If the office does not have oversight of an information technology or services contract, ensure that the state agency with oversight of the contract operates pursuant to section 24-37.5-105.4 regarding the delegation of authority; AND

(e) IF A CONTRACT PROVIDES ONGOING SERVICE AND DELIVERY TO COLORADANS, ENSURE THAT THE CONTRACT MAINTAINS CURRENT ARCHITECTURE DIAGRAMS THAT ARE UPDATED AT LEAST ANNUALLY.

**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), (2)(k), 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 TECHNOLOGY 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);

(j) SUBMIT TO THE JOINT TECHNOLOGY COMMITTEE, ON OR BEFORE NOVEMBER 1, 2027, 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;

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

(IV) A MITIGATION PLAN OR COMPENSATING CONTROLS FOR THE REMEDIATION OF EACH OPEN RECOMMENDATION MADE BY THE OFFICE OF THE STATE AUDITOR; AND

(k) (I) SUBMIT TO THE JOINT TECHNOLOGY COMMITTEE, ON OR BEFORE NOVEMBER 1, 2027, AND ON OR BEFORE NOVEMBER 1 OF EACH YEAR THEREAFTER, A WRITTEN STATEWIDE INFORMATION TECHNOLOGY SECURITY RISK REPORT THAT ASSESSES THE OVERALL SECURITY RISK POSTURE OF STATE AGENCY INFORMATION TECHNOLOGY SYSTEMS.

(II) TO SUPPORT THE PREPARATION OF THE SECURITY RISK REPORT REQUIRED BY SUBSECTION (2)(k)(I) OF THIS SECTION, THE CHIEF INFORMATION SECURITY OFFICER MAY CONDUCT EVALUATIONS OF STATE AGENCY INFORMATION TECHNOLOGY SYSTEMS AS THE CHIEF INFORMATION SECURITY OFFICER DEEMS NECESSARY, INCLUDING PENETRATION TESTING, VULNERABILITY SCANNING, CONFIGURATION EVALUATIONS, AND VENDOR AND SYSTEM REVIEWS.

(III) EACH STATE AGENCY SHALL PROVIDE TO THE CHIEF INFORMATION SECURITY OFFICER, UPON REQUEST, THE ACCESS AND INFORMATION NECESSARY TO CONDUCT EVALUATIONS PURSUANT TO SUBSECTION (2)(k)(II) OF THIS SECTION, INCLUDING SYSTEM ACCESS, PRODUCT INFORMATION, AND ARCHITECTURE INFORMATION.

(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. THE CHIEF INFORMATION OFFICER SHALL NOT DELEGATE THE DUTIES, RESPONSIBILITIES, OR POWERS OF THE CHIEF INFORMATION SECURITY OFFICER TO ANY PERSON OTHER THAN THE CHIEF INFORMATION SECURITY OFFICER. NOTHING IN THIS SECTION PREVENTS THE CHIEF INFORMATION SECURITY OFFICER FROM DIRECTING PERSONNEL WITHIN THE INFORMATION SECURITY OFFICE TO CARRY OUT SECURITY FUNCTIONS UNDER THE CHIEF INFORMATION SECURITY OFFICER'S SUPERVISION AND ACCOUNTABILITY. THE CHIEF INFORMATION SECURITY OFFICER IS RESPONSIBLE FOR THE ACCURACY OF THE COMPLIANCE REPORT REQUIRED IN SUBSECTION (2)(j) OF THIS SECTION AND THE SECURITY RISK REPORT REQUIRED IN SUBSECTION (2)(k) OF THIS SECTION, REGARDLESS OF WHICH PERSONNEL CONTRIBUTED TO THE PREPARATION OF THE REPORTS.

**SECTION 5. Act subject to petition - effective date.** This act takes effect at 12:01 a.m. on the day following the expiration of the ninety-day period after final adjournment of the general assembly (August 12, 2026, if adjournment sine die is on May 13, 2026); except that, if a referendum petition is filed pursuant to section 1 (3) of article V of the state constitution against this act or an item, section, or part of this act within such period, then the act, item, section, or part will not take effect unless approved by the people at the general election to be held in November 2026 and, in such case, will take effect on the date of the official declaration of the vote thereon by the governor.