



Fiscal Note

Legislative Council Staff

Nonpartisan Services for Colorado’s Legislature

SB 26-185: ENHANCE SECURITY OF OFFICE OF INFO TECH

Prime Sponsors:

Sen. Marchman; Baisley
Rep. Titone; Keltie

Fiscal Analyst:

Clayton Mayfield, 303-866-5851
clayton.mayfield@coleg.gov

Published for: Senate Business, Labor & Tech.

Drafting number: LLS 26-0979

Version: Initial Fiscal Note

Date: May 4, 2026

Fiscal note status: This fiscal note reflects the introduced bill, which was recommended by the Joint Technology Committee

Summary Information

Overview. The bill requires the Office of Information Technology to submit an information technology security compliance report to the Joint Technology Committee, allows the committee to request an audit, requires the office to develop a vendor contract list, and modifies other state information technology security procedures.

Types of impacts. The bill is projected to affect the following areas on an ongoing basis starting in FY 2026-27:

- State Expenditures

Appropriations. No appropriation is required.

**Table 1
State Fiscal Impacts**

Type of Impact	Budget Year FY 2026-27	Out Year FY 2027-28
State Revenue	\$0	\$0
State Expenditures (Cash Funds)	\$0	up to \$500,000
Transferred Funds	\$0	\$0
Change in TABOR Refunds	\$0	\$0
Change in State FTE	0.0 FTE	0.0 FTE

State expenditures are conditional upon the request of an audit and the submission of a budget request; they are assumed to be paid from the Technology Risk Prevention and Response Fund. Actual amounts and timing of expenditures may vary.

Summary of Legislation

The bill requires the Office of Information Technology (OIT) to submit an information technology (IT) security compliance report to the Joint Technology Committee (JTC), allows the JTC to request a special IT security audit, requires the OIT to develop a vendor contract list, and modifies other state IT security procedures as described below.

Security Compliance Report

The OIT must submit an IT security compliance report to the JTC by November 1, 2027, and by November each year thereafter. The report must include information on the OIT's compliance with applicable security standards, open recommendations from previous audits by the Office of the State Auditor (OSA), a timeline for remediation of open recommendations, and a mitigation plan for each open recommendation. Along with the compliance report, the OIT must also submit a statewide IT security risk report in coordination with other state agencies.

Joint Technology Committee Audit Request

The JTC may request that the Legislative Audit Committee (LAC) initiate a special information technology (IT) security audit by the Office of the State Auditor (OSA) within 91 days of receiving a technology security compliance report from the OIT. The JTC may request an audit if the report indicates that either an audit recommendation is unresolved for two or more years, or if there is a material discrepancy between the report and findings made in previous audits.

The OSA may contract with a third-party if an audit is approved. The OSA must obtain input from the OIT regarding the scope of the audit and consider the resources available to the OIT to reimburse audit costs. Reimbursement of audit costs may be paid from the Technology Risk Prevention and Response Fund (TRPR). Completed audits must be presented to the LAC first, and then made available to the JTC, the Joint Budget Committee, and the Governor.

Vendor Contract List

The OIT must develop a list of all active IT vendor contracts, and make this list available to state agency IT leadership and the JTC. State agencies must provide vendor information to the OIT. The bill requires that the OIT submit a one-time IT budget request to the JTC for the cost of developing the list, and may use the TRPR if more money is needed to implement and maintain the list.

Other State IT Security Procedures

The bill establishes requirements on the publication and implementation of technical IT standards developed by the OIT. The state's chief information officer is prohibited from delegating a duty, responsibility, or power of the chief information security officer (CISO) to

another individual, except that the CISO may direct work necessary to fulfill security responsibilities. State agencies must provide access and information necessary for the CISO to conduct security compliance and IT security risk reports.

Assumptions

The fiscal note assumes that costs for any special IT security audits are conditional upon a request by the JTC and approval by the LAC. Furthermore, it is assumed that the audit will be conducted through a third-party contract monitored by the OSA. If the JTC requests an audit as soon as it can, and the LAC approves, then the audit will begin sometime in 2027 and finish in FY 2027-28. The OSA will structure the contract with the input of the OIT, and that reimbursement will occur in FY 2027-28.

Regarding the vendor contract list, if additional resources are needed then the OIT will submit an IT budget request for consideration in late 2026. Approval of the request would provide funding for FY 2027-28.

Finally, the TRPR is assumed to cover costs for this bill, although other resources may be identified in the future.

State Expenditures

Starting in FY 2026-27, the bill increases workload and state expenditures in the OIT and the OSA, conditional upon the request of an audit by the JTC and the OIT requiring additional resources for the vendor contract list. It also may increase workload in other state agencies that receive services from the OIT.

Office of Information Technology

The OIT will reimburse the OSA for the costs of any audits requested and approved, which will increase expenditures for FY 2027-28. An audit of this kind is estimated to cost between \$250,000 and \$500,000, depending on the scope of work identified.

The OIT will also have additional workload to develop the vendor contract list. At this time, it is estimated that the OIT can accomplish this work using existing resources. However, if additional appropriations are required, it is assumed that OIT will request funds through the annual budget process.

Other duties required by the bill, including creating the compliance report and coordinating with other state agencies will generate a minimal increase in workload. No change in appropriations is required.

Legislative Department

Workload will increase for the OSA to contract for an audit, and monitor the contract. This increase is expected to be minimal, and no change in appropriations is required.

Other State Agencies

Workload will increase for agencies that receive services from the OIT to coordinate the collection of information necessary for the OIT to produce a vendor contract list and complete reports required by the bill. The fiscal note assumes this increase will be minimal, and no change in appropriations is required.

Effective Date

The bill takes effect 90 days following adjournment of the General Assembly sine die, assuming no referendum petition is filed.

State and Local Government Contacts

Information Technology

State Auditor