

Fiscal impact reports (FIRs) are prepared by the Legislative Finance Committee (LFC) for standing finance committees of the Legislature. LFC does not assume responsibility for the accuracy of these reports if they are used for other purposes.

FISCAL IMPACT REPORT

SPONSOR	<u>Senate Rules Committee</u>	LAST UPDATED	<u>2/28/2025</u>
		ORIGINAL DATE	<u>2/28/2025</u>
SHORT TITLE	<u>Cybersecurity Act & Office Changes</u>	BILL	<u>CS/Senate Bill</u>
		NUMBER	<u>254/SRCS</u>
		ANALYST	<u>Hilla</u>

ESTIMATED ADDITIONAL OPERATING BUDGET IMPACT*

(dollars in thousands)

Agency/Program	FY25	FY26	FY27	3 Year Total Cost	Recurring or Nonrecurring	Fund Affected
Office of Cybersecurity	No fiscal impact	\$6.4 to \$13.6	\$6.4 to \$13.6	\$12.8 to \$27.2	Recurring	General Fund

Parentheses () indicate expenditure decreases.

*Amounts reflect most recent analysis of this legislation.

Relates to House Bill 2 and House Bill 60

Sources of Information

LFC Files

Agency Analysis Received From

Administrative Office of the Courts (AOC)
Department of Information Technology (DoIT)
Office of Broadband Access and Expansion (OBAE)
New Mexico Attorney General (NMAG)
Department of Health (DOH)
Health Care Authority (HCA)
Department of Public Safety (DPS)
Public Education Department (PED)
Homeland Security and Emergency Management Department (DHSEM)

Agency Analysis was Solicited but Not Received From

New Mexico Supreme Court

SUMMARY

Synopsis of SRC Substitute for Senate Bill 254

The Senate Rules Committee Substitute for Senate Bill 254 (SB254) amends Section 9-27A-3 NMSA 1978, the Cybersecurity Act, to change the name of the Cybersecurity Office to the Office of Cybersecurity (OCS). Additionally, SB254 allows the Office of Cybersecurity to develop minimum cybersecurity controls for managing and protecting information technology assets and infrastructure for all entities connected to a state-operated or state-owned telecommunications network, defined as a network controlled by the Department of Information Technology (DoIT). SB254 amends Section 9-27A-5 NMSA 1978 to add the following to the

Cybersecurity Advisory Committee:

- One member appointed by the chief justice of the Supreme Court; and
- Four members appointed by the governor, in consultation with the secretary of DoIT and the state chief information security officer, who satisfy any federal or state cybersecurity grant funding requirements, individually or collectively.

This bill does not contain an effective date and, as a result, would go into effect 90 days after the Legislature adjourns if enacted, or June 20, 2025.

FISCAL IMPLICATIONS

Public members of the new cybersecurity advisory council or subgroup established by the bill may receive per-diem and mileage reimbursement in accordance with Sections 10-8-1 through 10-8-8 NMSA 1978 (the Per Diem and Mileage Act). Mileage costs would vary widely and are difficult to estimate. The Per Diem and Mileage Act allows \$45 per member should meetings be less than four hours a day, and \$95 per member should meetings last longer than four hours. This creates a range of \$540-\$1,140 a month for all 12 members depending on the length of the meeting. This creates an estimated fiscal impact of \$6.4 thousand to \$13.6 thousand for the 12-member committee for a year's worth of meetings.

SIGNIFICANT ISSUES

Both the Legislature and the executive have taken steps to centralize and standardize cybersecurity initiatives across public institutions in the state. In 2023, the Legislature created the Cybersecurity Office, which now operates as administratively attached to the Department of Information Technology (DoIT). The office currently provides cybersecurity services to executive agencies, counties, tribal entities, municipalities, higher education institutions, and public-school districts. Additionally, a 2024 executive order directed DoIT to conduct information technology and security assessments on executive agencies to detect vulnerabilities and support mitigation efforts as necessary.

DoIT states that a 2022 executive order created a separate Cybersecurity Planning Committee, which has duplicated and overlapping responsibilities with the Cybersecurity Advisory Committee created by the Cybersecurity Act. DoIT states that SB254 would eliminate duplication efforts between the two committees and streamline performance.

DoIT reports that 76 executive agencies are under its statewide cyber scanning service and attack surface management, with no judicial or legislative agencies under the current Cybersecurity Office's purview. DoIT states that many public and private entities, including vendors and municipalities, use the state IT network, however, it is unclear who would be subject to the new OCS' minimum cybersecurity standards as the bill currently stands. The Office of Broadband Access and Expansion (OBAE) notes that "state-operated or state-owned telecommunications network" are not defined in SB254, which makes what is subject to OCS's minimum cybersecurity standards unclear.

The Department of Public Safety (DPS) and the Administrative Office of the Courts (AOC) note that the Cybersecurity Advisory Committee does not include a law enforcement representative.

Both DPS and AOC suggest that DPS should be added to the advisory committee to ensure statewide cybersecurity policies are consistent with the federal standards that all state, local, tribal and federal criminal justice agencies already comply with. DPS adds that OCS could leverage existing channels through DPS to communicate with counties and municipalities during cybersecurity incidents. Having some law enforcement representations is critical, especially considering a previous cyberattack in 2024 on a state agency that affected various law enforcement agencies.

DoIT states that the change of Cybersecurity Office to the Office of Cybersecurity would ensure that the office follows other naming conventions for other administratively attached agencies and will help identify the status of the cybersecurity function within DoIT.

AOC suggests adding “a private sector cybersecurity expert or employed by a business offering cybersecurity services, provided the business is not performing services for the state or otherwise engaged in business with the state.”

The Department of Health suggests adding the words “confidentiality” and “transmitted” to Section 1 (B) (1).

CONFLICT, DUPLICATION, COMPANIONSHIP, RELATIONSHIP

SB254 relates to appropriations in House Bill 2, which includes both recurring and nonrecurring appropriations to DoIT for cybersecurity, and House Bill 60, which creates the Artificial Intelligence Act.

TECHNICAL ISSUES

SB254’s amendment in Section 1 (B) (1) would allow OCS to develop minimum cybersecurity controls for managing and protecting information technology assets for “all entities that are connected to a state-operated or state-owned telecommunications network” contradicts Section 2 (E) of the Act. However, Section 2 (E) explicitly states “compliance with those guidelines or recommendations by non-executive agencies or county, municipal or tribal governments shall be strictly voluntary [emphasis added].” Should SB254’s intent be to require all entities, not just executive agencies, that are connected to a state-operated or state-owned telecommunications network adhere to OCS guidelines, the language in Section 2 (E) renders this moot.

EH/rl/hj/SL2