FISCAL IMPACT REPORT

SPONSOR Padilla/Sariñana **LAST UPDATED** **ORIGINAL DATE** 2/14/2025

SHORT TITLE Cybersecurity Act & Office Changes **BILL NUMBER** Senate Bill 254

ANALYST Hilla

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)

Agency Analysis was Solicited but Not Received From
Homeland Security and Emergency Management Department (DHSEM)
New Mexico Supreme Court

SUMMARY

Synopsis of Senate Bill 254

Senate Bill 254 (SB254) amends Section 9-27A-3 NMSA 1978, the Cybersecurity Act, to change the name of the Cybersecurity Office as 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. 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 who is experienced with cybersecurity issues;
- A member of the Legislature appointed by the New Mexico Legislative Council who is familiar with cybersecurity issues;
- Four members appointed by the governor who have experience with cybersecurity issues, provided that at least one appointee be an educator or employed by an education institution; a health care provider or employed by a health care provider; employed by the New Mexico Homeland Security and Emergency Management Department; and a private sector cybersecurity expert of employed by a business offering cybersecurity services.

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.

SB254 adds new members to the Cybersecurity Advisory Committee. For all members except for a member of the Legislature, language is explicit that the new member is someone "experienced" with cybersecurity issues, whereas the member from the legislature is someone who is "familiar" with cybersecurity issues.

The New Mexico Attorney General (NMAG) states that the way the bill currently presents, it is read that the chief justice of the supreme court is the person who should be experienced with cybersecurity issues, not the member appointed by the justice.

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." Should SB254's intent require all entities that are connected to a state-operated or state-owned telecommunications network, this addition is moot due to the language in Section 2 (E) DoIT states that the addition of Section 1 (B) grants OCS authority over all branches of government and non-agency users; however, this is not the case given the language

in Section 2 (E).

Additionally, NMAG notes:

> The revision in Subsection (B)(7) in Section 2 requires at least one of the Governor's 4 appointees "shall be: (a) an educator or employed by an education institution; (b) a health care provider or employed by a health care provider; (c) employed by the homeland security and emergency management department; ***and*** (d) a private sector cybersecurity expert or employed by a business offering cybersecurity services." (Emphasis added.) While it may be possible for all four categories to exist in one person, it is exceedingly unlikely. It seems more likely that the bill intends that at least one appointee is *one* of the four identified persons. Replacing the emphasized "and" with "or" would address this.

EH/rl