LFC Requester:	Hilla

AGENCY BILL ANALYSIS - 2025 REGULAR SESSION

WITHIN 24 HOURS OF BILL POSTING, UPLOAD ANALYSIS TO
AgencyAnalysis.nmlegis.gov and email to **billanalysis@dfa.nm.gov**
(Analysis must be uploaded as a PDF)

SECTION I: GENERAL INFORMATION

{Indicate if analysis is on an original bill, amendment, substitute or a correction of a previous bill}

Date Prepared: 2/4/25 *Check all that apply:*
Bill Number: SB 254 Original ____ Correction ____
Amendment ____ Substitute _X___

Sponsor:	Sen. Michael Padilla	**Agency Name and Code Number**:		NM DoIT - 361	
Short Title:	Cybersecurity Act & Office Changes	**Person Writing Analysis:**		Raja Sambandam	
		Phone:	505-660-3280	**Email:**	Raja.sambandam@cyber.nm.gov

SECTION II: FISCAL IMPACT

APPROPRIATION (dollars in thousands)

Appropriation		Recurring or Nonrecurring	Fund Affected
FY25	**FY26**		
0	0	0	0

(Parenthesis ( ) indicate expenditure decreases)

REVENUE (dollars in thousands)

Estimated Revenue			Recurring or Nonrecurring	Fund Affected
FY25	**FY26**	**FY27**		
0	**0**	**0**	0	0

(Parenthesis ( ) indicate revenue decreases)

ESTIMATED ADDITIONAL OPERATING BUDGET IMPACT (dollars in thousands)

	FY25	FY26	FY27	3 Year Total Cost	Recurring or Nonrecurring	Fund Affected
Total						

(Parenthesis ( ) Indicate Expenditure Decreases)

Duplicates/Conflicts with/Companion to/Relates to:
Duplicates/Relates to Appropriation in the General Appropriation Act

SECTION III: NARRATIVE

BILL SUMMARY

Synopsis: The Senate Rules Committee (SRC) substitute for Senate Bill (SB) 254 proposes to amend the Cybersecurity Act (SB280) that was passed during the 2023 regular session and codified in Chapter 9, Article 27A NMSA 1978 (the "Cybersecurity Act")

Section 1 of the SRC substitute would add a new definition for "state-operated or state-owned telecommunications network" which would mean "a telecommunications network controlled by the department of information technology pursuant to the Department of Information Technology Act."

Section 2 would change the name of the Cybersecurity Office to the Office of Cybersecurity. This amendment is replicated for every instance of "Cybersecurity Office" in the Cybersecurity Act.

Section 2 would also amend Section 9-27A-3(B)(2) to clarify that the Office of Cybersecurity can regulate connections to "a state-operated or state-owned telecommunications network". Current law specifies that the Office can only regulate connections to an agency owned or operated network.

Section 3 of the SRC substitute for SB254 would amend 9-27A-5(A) to change the composition of the Cybersecurity Advisory Committee ("Advisory Committee") as follows:

• Make the state chief information security officer (CISO) a voting member of the Advisor Committee, except on matters pertaining to the hiring, firing, compensation or discipline of the CISO.

• One member appointed by the Chief Justice of the Supreme Court, without further qualification.

• Decrease the number of members appointed by the New Mexico Municipal League from three to two.

• Decrease the number of members appointed by the New Mexico Association of Counties from three to two.

• Increase the number of members appointed by the Governor from three to four, and requiring

those appointments to be made in consultation with the secretary of information technology and the state chief information security officer; provided that these members, individually and collectively, shall enable the committee to satisfy any federal or state cybersecurity grant funding requirements.

FISCAL IMPLICATIONS

None for DoIT.

SIGNIFICANT ISSUES

The Cybersecurity Office is administratively attached to the Department of Information Technology (DoIT). The Office of Broadband Access and Expansion is also administratively attached to DoIT. Changing the name of the Cybersecurity Office to the "Office of Cybersecurity" would ensure that cybersecurity function follows the same naming convention as Office of Broadband. This is a common naming convention for administratively attached agencies, e.g., Office of Policy and Planning, and Office of Elder Affairs. Following the established naming conventions will help avoid confusion as to the identity and status of the cybersecurity function within DoIT.

New Mexico currently has two committees responsible for state cybersecurity planning. The Cybersecurity Act created the Cybersecurity Advisory Committee. Executive Order 2022-141 created the Cybersecurity Planning Committee. The functions of these two bodies overlap significantly, resulting in an inefficient, duplicative use of state cybersecurity expertise. This can also result in potential conflicts in state cybersecurity policy. However, only the Planning Committee is composed of members who enable the state to qualify for federal cybersecurity grant funding under the State and Local Cybersecurity Grant Program (SLCGP).

By (1) adding the requirement that the Governor's appointees shall occupy a role or position that will enable the committee to satisfy any federal or state cybersecurity grant funding requirements, (2) making the State CISO a voting member, and (3) increasing the number of members the Governor can appoint from three to four, the Governor can configure the committee to meet the requirements for SLCGP funding. By not specifying roles or positions that the Governor's appointees must hold outside of the Advisory Committee, the Governor has the flexibility to compose the Committee to meet the requirements of current and future grant funding requirements. If there are no relevant grant program requirements, the flexibility would enable the Governor to appoint representatives of stakeholders who would best compliment other appointees and enable the Committee to best serve the varied public sectors impacted by its work.

After the Advisory Committee is configured to support SLCGP funding requirements, the Governor can retire the Planning Committee. That will ensure that the state cybersecurity policy is established by a single governing statutory body. The SRC substitute would also give the judicial branch expanded discretion on whom to appoint to the Advisory Committee.

The Cybersecurity Act allows the Cybersecurity Office to specify cybersecurity protections that must be implemented by an "agency" user of the state information technology network.

However, many other public and private entities, including vendors and municipalities, use the state IT network. Whether a user of the network is public or private, an agency or a municipality, the state should be able to require cybersafe practices for network use.

The Office of Broadband Access and Expansion ("OBAE") operates the State Education Network. The SEN may only be used to support education. Because the SEN is currently self-contained, OBAE was concerned that by giving the Office authority over state networks, or agency operated networks that are separate from the DoIT network, the Office would have authority over the SEN in contravention of federal law. To eliminate that concern, OBAE proposed adding a definition that clarifies that a "state-operated or state-owned telecommunications network" means a telecommunications network controlled by DoIT pursuant to the DoIT Act. This definition would not include the SEN, or any other self-contained network operated by a public entity. This clarification in authority would allow the Cybersecurity Office to establish cybersecurity controls to protect the DoIT network and to secure connections to that network but would not allow the office to regulate cybersecurity for independent networks outside of DoIT's control.

PERFORMANCE IMPLICATIONS

By aligning the Cybersecurity Advisory Committee with the SLCGP requirements and allowing the Governor to retire the Cybersecurity Planning Committee, the Cybersecurity Office will be able to eliminate duplication of efforts which are currently occurring between the two committees, thereby streamlining performance.

ADMINISTRATIVE IMPLICATIONS

CONFLICT, DUPLICATION, COMPANIONSHIP, RELATIONSHIP

TECHNICAL ISSUES

OTHER SUBSTANTIVE ISSUES

ALTERNATIVES

WHAT WILL BE THE CONSEQUENCES OF NOT ENACTING THIS BILL

Status quo, which would perpetuate nearly duplicative cybersecurity policy committees, and ambiguity as to which agency has authority to regulate non-agency use of the state IT network that is operated by DoIT.

AMENDMENTS