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
Bill Number: SB 254

Check all that apply:
Original _x___ Correction ____
Amendment ____ Substitute ____

Sponsor: Sen. Michael Padilla
Agency Name and Code Number: NM DoIT - 361
Person Writing Analysis: Raja Sambandam
Short Title: Cybersecurity Act & Office Changes
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: 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 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 1 would also amend Section 9-27A-3(B)(2) to clarify that the Office of Cybersecurity can regulate connections to the State's information technology network by any user. Current law specifies that the Office can only regulate connections by agency users of the state network.

Section 2 of the SB254 would amend 9-27A-5(A) to change the composition of the Cybersecurity Advisory Committee ("CAC") as follows:

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

• 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 members to be representatives from education, health, emergency management and private sectors, and experienced with cybersecurity.

FISCAL IMPLICATIONS

None for DoIT.

Note: major assumptions underlying fiscal impact should be documented.

Note: if additional operating budget impact is estimated, assumptions and calculations should be reported in this section.

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 satisfy the federal State and Local Cybersecurity Grant Program (SLCGP) funding requirements. By adding members from the education, health and private sectors to the Advisory Committee, and making the State CISO a voting member of that committee, the Advisory Committee would meet the requirements for the SLCGP. This would allow the Governor to retire the Planning Committee and ensure that state cybersecurity policy is established by a single governing statutory body.

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 proposed revisions to the Cybersecurity Act would give the Cybersecurity Office explicit regulatory authority over the use of the state-owned IT network for both agency and non-agency users.

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.

AMENDMENTS