LFC Requester:

AGENCY BILL ANALYSIS
2024 REGULAR SESSION

WITHIN 24 HOURS OF BILL POSTING, UPLOAD ANALYSIS TO:

Analysis.nmlegis.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}

Check all that apply:
Original ___ **Amendment** ___
Correction ___ **Substitute** X

Date 1/31/2024
Bill No: SB 129s

Sponsor: Michael Padilla & Debra M. Sariñana
Short Title: Cybersecurity Act

Agency Name and Code Number: 790-Department of Public Safety
Person Writing Kent Augustine
Phone: 505-709-5264 **Email** kent.augustine@dps.nm.gov

SECTION II: FISCAL IMPACT

APPROPRIATION (dollars in thousands)

Appropriation		Recurring or Nonrecurring	Fund Affected
FY24	**FY25**		
0.0	0.0		

(Parenthesis ( ) Indicate Expenditure Decreases)

REVENUE (dollars in thousands)

Estimated Revenue			Recurring or Nonrecurring	Fund Affected
FY24	**FY25**	**FY26**		
0.0	0.0	0.0		

(Parenthesis ( ) Indicate Expenditure Decreases)

ESTIMATED ADDITIONAL OPERATING BUDGET IMPACT (dollars in thousands)

	FY24	FY25	FY26	3 Year Total Cost	Recurring or Nonrecurring	Fund Affected
Total	NFI	NFI	NFI	NFI		

(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

SHPAC Substitute for SB0129 dated January 30, 2024, retains the intent and most of the major provisions in the original bill. Major differences between the two include membership on the Cybersecurity Advisory Committee; approval authority over cybersecurity and information security projects; authority over emergency procurements; and issuance of orders to protect the state's digital assets from imminent threat.

Specifically, the substitute version:

- Eliminates application to entities transacting business with the state;
- Empowers Cybersecurity Office to conduct security assessments (instead of audits) to detect security vulnerability incidents;
- Empowers Cybersecurity Office to approve agency cybersecurity, as well as information security, RFPs and invitations for bids;
- Drops Cybersecurity Office authority to approve emergency procurement but directs agencies to consult with the Office and immediately transmit notice of the procurement to the Office;
- Replaces authority to approve all cybersecurity legislative appropriation requests of $25 million or more with authority to approve all requests of agencies related to cybersecurity and information security projects incorporating protection of personal, sensitive, or confidential information as defined by the Office; also, extends this authority to approval of requests by county, municipal, public school and higher education institutions;
- Allows the Security Officer to issue orders necessary to protect the state's digital assets from imminent threat.
- Drops the Secretary of Information Technology from membership in the Cybersecurity Advisory Committee;
- Restores to three the number of Cybersecurity Advisory Committee members appointed by the New Mexico Association of Counties and New Mexico Municipal League and cuts to two the members appointed by the Governor, both of whom must have experience with

cybersecurity issues one for public education institutions and the other for public health institutions; no members are appointed by the Security Officer.

FISCAL IMPLICATIONS
None to DPS.

SIGNIFICANT ISSUES
Section 3. B. Outlines the membership of the Cybersecurity Advisory Committee. A significant omission of the committee is the FBI designated Criminal Justice Information Services (CJIS) Information Security Officer (ISO) for the State of New Mexico. The CJIS ISO has specific cybersecurity duties, responsibilities, and powers granted by the FBI through the CJIS Security Policy. All state, local, tribal, and federal criminal justice agencies are governed by the CJIS Security Policy. The FBI designates one agency in each state and territory as the CJIS Systems Agency (CSA). The New Mexico CSA is DPS. Each CSA must have a CJIS Systems Officer (CSO) and a CJIS ISO.

The committee, and the State would significantly benefit by having the CJIS ISO as a permanent voting member on the committee for the following reasons:

1. As outlined in the bill, there is no representation on the committee of law enforcement. The CJIS ISO oversees the unique aspects of cybersecurity across all law enforcement agencies operating in New Mexico.

2. The CJIS ISO undergoes significant training by the FBI on cybersecurity best practices, and policies. The CJIS ISO must attend the annual CJIS ISO Symposium along with all other CJIS ISOs where they meet with the FBI's CJIS division leadership, attend training, share ideas, and build relationships. These trainings and relationships provide the CJIS ISO with unique perspectives and added resources not provided to anyone else in New Mexico.

3. The CJIS ISO has established network and communication channels to communicate with every criminal justice agency operating in New Mexico. These channels are designed to get messaging out to all New Mexico criminal agencies within minutes. These channels can be a significant point of leverage when the Cybersecurity Office needs to communicate to counties and municipalities during cybersecurity incidents.

4. The CJIS ISO along with the CSO have the authority to set mandatory policies that all criminal justice agencies must follow. These policies can be tailored to each state. The CJIS ISO and CSO have the authority to audit any criminal justice agency. The CJIS ISO and CSO have the authority to sanction criminal justice agencies for not adhering to the CJIS Security Policy. This authority, granted by the FBI through the CJIS Security Policy, are unique and would provide the committee and the New Mexico Chief Information Security Officer a means to enforce policies on agencies that otherwise are not under the jurisdiction of the Cybersecurity Office.

The omission of the CJIS ISO from the membership of the committee is a lost opportunity in having a voice of law enforcement in the room, as well as the resources the CJIS ISO can provide the committee including communications channels, relationships, FBI training, and the authority to enforce cybersecurity standards and policies on agencies not otherwise under the jurisdiction of the State.

PERFORMANCE IMPLICATIONS
None to DPS.

ADMINISTRATIVE IMPLICATIONS
None to DPS.

CONFLICT, DUPLICATION, COMPANIONSHIP, RELATIONSHIP
None.

TECHNICAL ISSUES
None to DPS.

OTHER SUBSTANTIVE ISSUES
None to DPS.

ALTERNATIVES
None.

WHAT WILL BE THE CONSEQUENCES OF NOT ENACTING THIS BILL
Status quo will remain.

AMENDMENTS
None proposed.