LFC Requester:	Emily Hilla

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 X **Amendment** ____
Correction ___ **Substitute** ____

Date 1-26-2024
Bill No: SB 129

Sponsor: Sen. Michael Padilla
Rep. Debra M. Sarinana
Short Title: Cybersecurity Act Changes

Agency Name and Code Number: Dept. of Information Technology – 36100
Person Writing: Raja Sambandam
Phone: 505-660-3280 **Email** raja.sambandam@doit.nm.gov

SECTION II: FISCAL IMPACT

APPROPRIATION (dollars in thousands)

Appropriation		Recurring or Nonrecurring	Fund Affected
FY24	**FY25**		
-0-	-0-	n/a	n/a

(Parenthesis ( ) Indicate Expenditure Decreases)

REVENUE (dollars in thousands)

Estimated Revenue			Recurring or Nonrecurring	Fund Affected
FY24	**FY25**	**FY26**		
-0-	**-0-**	**-0-**	n/a	n/a

(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	-0-	-0-	-0-	-0-	n/a	n/a

(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 129 ("SB129") amends the Cybersecurity Act as follows:

- Clarifies that the rules establishing minimum security standards and policies are applicable to entities receiving general fund appropriations and persons or entities transacting business with the state.
- Enacts a new provision that the rules establishing minimum security standards shall include a requirement that entities receiving general fund appropriations from the legislature shall report to the cybersecurity office all information technology and cybersecurity expenditures in a form and manner established by the cybersecurity office.
- Provides for rulemaking in areas where the Cybersecurity Act previously only required the establishment of controls, policies, standards, or processes.
- Provides that the cybersecurity office shall: approve agency information technology requests for proposals and other agency requests that are subject to the Procurement Code, prior to final approval; approve agency cybersecurity and information security contracts and amendments to those contracts, including emergency procurement, sole contracts and price agreements, prior to final approval; and review and approve all agency, public school, higher education institution, county and municipality legislative appropriation requests of twenty-five million dollars ($25,000,000) or more related to cybersecurity and information security prior to submission of such appropriation requests to the legislature.
- Clarifies that the security officer may issue orders regarding the compliance of agencies with rules, policies, standards, or controls issued by the cybersecurity office in addition to the security officer's existing authority to issue orders regarding compliance with guidelines or recommendations of the cybersecurity advisory committee.
- Enacts a new requirement that public bodies not subject to the jurisdiction of the security officer shall adopt and implement cybersecurity, information security and privacy policies, standards and procedures based upon frameworks and minimum standards issued by the national institute of standards and technology.
- Amends the provisions relating to creation of the cybersecurity advisory committee to establish that the security officer is a voting member of the committee and modifies the membership of the committee.

FISCAL IMPLICATIONS

SB129 does not contain an appropriation.

SIGNIFICANT ISSUES

Clarifying that the rules establishing minimum security standards and policies are applicable to entities receiving general fund appropriations and persons or entities transacting business with the state is necessary to fully defend and protect the state's IT infrastructure from cybersecurity attacks and related information security incidents. Failure to require implementation of minimum security standards of some entities on the state IT infrastructure leaves vulnerabilities that could impact all entities on that infrastructure.

Permitting the cybersecurity office to establish controls, policies, standards, or processes through rulemaking provides for a more interactive and transparent public process that allows the persons and entities affected by the rules to participate in their creation.

Requiring the cybersecurity office to review and approve cybersecurity-related procurements, contracts and legislative appropriation requests is similar to the secretary's authority under the Department of Information Technology Act and interjects a level of expertise and experience into the procurement and appropriations process to help ensure each complies with current and established cybersecurity standards, policies and best practices.

Providing the cybersecurity office with authority to issue orders regarding compliance with rules, policies, standards and controls issued by the cybersecurity office ensures that the security officer can seek accountability not only for compliance with the federal and state requirements but also with cybersecurity advisory committee's guidelines and standards established by the cybersecurity office.

Requiring public bodies not subject to the jurisdiction of the cybersecurity office to adopt and implement cybersecurity, information security and privacy policies, standards and procedures based upon frameworks and minimum standards issued by the national institute of standards and technology provides those public bodies a set of cybersecurity activities, desired outcomes and applicable informative references common across critical infrastructure sectors and offers minimum standards that those public bodies shall adopt to protect their own IT infrastructure.

Modifying the membership of the cybersecurity advisory committee ensures compliance with the Federal Notice of Funding Opportunity requirements necessary to apply for and receive cybersecurity-related grants and other funding.

ADMINISTRATIVE IMPLICATIONS

Additional staffing would be needed to review and approve cybersecurity and information security procurements, contracts, and legislative appropriation requests. However, these needs were taken into consideration and are addressed in the Cybersecurity Office's budget request.

AMENDMENTS

Amend Section 9-27A-3(B)(1) of the bill to delete the strikethrough: adopt and implement rules establishing minimum security standards and policies applicable to entities receiving general fund appropriations ~~and persons or entities transacting business with the state~~ to protect state information technology systems and infrastructure and provide appropriate governance and application of the standards and policies across state information technology resources to promote the availability, security and integrity of the information processed, transacted or stored in the state's information technology infrastructure and systems. The rules shall include a requirement that entities receiving general fund appropriations from the legislature shall report to the cybersecurity office all ~~information technology and~~ cybersecurity and information security expenditures in a form and manner established by the cybersecurity office;

Amend Section 9-27A-3(B)(13) of the bill to delete the strikethrough and insert the underlined: approve agency ~~information technology~~ cybersecurity and information security requests for proposals and ~~other agency requests~~ invitations for bids that are subject to the Procurement Code, prior to final approval;

Amend Section 9-27A-3(B)(14) of the bill to delete the strikethrough and insert the underlined: approve agency cybersecurity and information security contracts and amendments to those contracts, including ~~emergency procurement,~~ sole source contracts and price agreements, prior to final approval. An agency that intends to make a cybersecurity or information security emergency procurement shall consult with the cybersecurity office and promptly thereafter transmit notice of final procurement to the cybersecurity office; and

Amend Section 9-27A-3(B)(15) of the bill to delete the strikethrough and insert the underlined: "review and approve all agency, public school, higher education institution, county and municipality legislative appropriation requests ~~of twenty-five million dollars (25,000,000) or more~~ related to cybersecurity or information security projects that incorporate the protection of personal, sensitive and confidential information prior to submission of such appropriation requests to the legislature."

Amend Section 9-27A-3(C) of the bill to insert the underlined and delete the strikethrough: "Pursuant to the Cybersecurity Act or other statutory authority, the security officer may issue orders regarding the compliance of agencies with rules, policies, standards or controls issued by the cybersecurity office and guidelines or recommendations of the cybersecurity advisory committee, and orders necessary to protect the state's digital assets from imminent threat. Compliance with ~~orders, rules, policies, standards, controls, guidelines or recommendations by the cybersecurity office or the cybersecurity advisory committee~~ the orders listed above shall be voluntary for county, municipal or tribal governments.

Amend Section 9-27A-4(B) of the bill after the first semicolon to insert the underlined and delete the strikethrough: provided that the security officer shall be recused from deliberations and voting on matters concerning supervision, discipline or compensation of the security officer and the ~~secretary of information technology or the secretary's designee~~ cybersecurity advisory committee shall determine a member to chair those deliberations and votes.

Amend Section 9-27A-4(B) of the bill to delete subsections (1) and (2).

Amend Section 9-27A-4(B)(6) of the bill to delete “two” and insert “three”.

Amend Section 9-27A-4(B)(7) of the bill to delete “two” and insert “three”.

Amend Section 9-27A-4(B)(8) of the bill to delete the strikethrough and insert the underlined: three members appointed by the governor ~~who may represent separate agencies other than the department of information technology and are experienced with cybersecurity issues~~ including the secretary of the department of homeland security and emergency management or the secretary’s designee, one member who has experience with cybersecurity issues for public education institutions, and one member who has experience with cybersecurity issues for public health institutions;

Amend Section 9-27A-4(B) of the bill to delete subsections (9) and (10).