| 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** x **Amendment** ___
**Correction** ___ **Substitute** ___

**Date** 1/24/2024
**Bill No**: SB 129

**Sponsor:** M. Padilla; D. Sarinana
**Short Title:** CYBERSECURITY ACT CHANGES

**Agency Name and Code Number**: Department of Finance and Administration-341
**Person Writing** Joseph R. Baros, Jr.
**Phone:** (505)795-4870 Joseph.Baros@dfa.nm

**SECTION II: FISCAL IMPACT**

**APPROPRIATION (dollars in thousands)**

| Appropriation | | Recurring or Nonrecurring | Fund Affected |
|---|---|---|---|
| **FY24** | **FY25** | | |
| | Unknown | Recurring | |
| | | | |

(Parenthesis ( ) Indicate Expenditure Decreases)

**REVENUE (dollars in thousands)**

| Estimated Revenue | | | Recurring or Nonrecurring | Fund Affected |
|---|---|---|---|---|
| **FY24** | **FY25** | **FY26** | | |
| | | | | |
| | | | | |

(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 | Unknown | Unknown | Unknown | Recurring | |

(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:

SB129 Cyber Security Act Changes, amends the existing Cybersecurity Act to: (1) clarify the scope of the rules establishing minimum security standards so the rules apply to *entities receiving general funds appropriations and persons or entities transacting business with the stat*e; (2) impose reporting requirements on entities receiving general funds appropriations and persons or entities transacting business within the state; (3) provide authority to the Cybersecurity Office to conduct information technology and security audits; (4) give authority to the Cybersecurity Office to review and approve agency information technology requests for proposals and other agency requests that are subject to the Procurement Code; (5) provide authority to the Cybersecurity Office to create standards related to responses to cyber incidents, review and approve all technology related proposals, including contracts, amendments, and emergency procurements; (6) provide authority to the Cyber Security Office to 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; and (7) provide authority to the Cybersecurity Office to review and approve all agency, public schools, higher education institutions, county and municipalities legislative appropriation requests over $25M; and (8) provide authority to the Cybersecurity Office to issue orders to agencies for compliance of rules, policies, standards and guidelines created by and implemented by the cybersecurity advisory committee. Public bodies not subject to the jurisdiction of the cybersecurity information officer must adopt policies and standards that comply with minimum requirements of the National Institute of Standards and Technology (NIST).

SB129 further clarifies that the Security Officer, or designee, is a voting member, except for matters and deliberations concerning supervision, discipline, or compensation of the security officer, which shall be reserved for the Secretary of the Information Technology, or designee. SB129 also adds the Secretary of Homeland Security and Emergency Management to advisory committee. The Act adds requirements of members for advisory committee from public education institutions and public health institutions with experience in the areas of cybersecurity. It removes security officers' authority to issue orders of compliance pursuant. to the Act to non-executive agencies, county, municipal, higher education entities, or tribal

entities.

**FISCAL IMPLICATIONS:**

The proposed legislation has an unknown fiscal impact. This is due to no requirements or standards for completing a security audit. SB129 doesn't specify who will pay for cybersecurity audits for the Department of Information Technology, Cybersecurity Office, or the agency. Impact on procurement will delay expenditures and may increase costs as quotes and market prices will fluctuate based on the supply and demand of goods and services. This does consider statewide price agreements as some include terms of open market value. The Cybersecurity office should consider providing grants to entities to cover the increased cost of implementing rules noted in SB129. This could also be done by adding a baseline increase to all IT appropriations to cover these costs.

SIGNIFICANT ISSUES: Additional agency reporting requirements on all technology and cybersecurity purchases to the Cybersecurity Office in a manner or form developed and approved by them. SB129 grants power to issue orders and act concerning issues against agencies regarding compliance with rules, regulations and orders issues by the Cybersecurity Office and advisory committee. It requires additional review and approval of all procurements not only related to cybersecurity but expanded language grant ability, authority and approval of the Cybersecurity Office for all technology related purchases. SB129 further grants the Cybersecurity Office the authority, prior to final approval, the ability to review, amend, and approve agency contracts, amendments, requests for proposals or any purchase and related documentation covered under the State Procurement Code. SB129 grants review and approval authority to the Cybersecurity Office related to agency, higher education institutions, county and municipality legislative appropriations over $25M or any appropriation request related to cybersecurity or information security. The Cybersecurity Office requires additional audits outside of scans and penetration testing and reviews currently being done the Department of Information Technology (DoIT) with Ivanti. Are these additional audits at the expense of the agency or rolled into costs currently charge by DoIT? Addition of designee to act on behalf of Security Officer on Advisory committee is acceptable; however, language only excludes Security Officer from voting on compensation, disciplinary action or supervision. The act does not exclude Security Officers designee from voting thus creating a potential conflict. The act also identifies member of the Department of Homeland Security and Emergency Management (DHSEM) to advisory board. Authority for cybersecurity oversight in coordination with the federal government resides with the Department of Public Safety (DPS) not DHSEM.

**PERFORMANCE IMPLICATIONS:** Additional reviews of purchases and contracts may delay the procurement process by introducing additional. Purchases require approval by the agency and DFA. Any contracts and amendments related to IT purchases are required to be reviewed by the Department of Information Technology Enterprise Project Management Office DoIT-EPMO). Once reviewed and approved by EMPO, and contingent upon funding and any additional requirements set forth by the EMPO, contacts and amendments are submitted as per procurement process to General Services Division Contract Review Bureau for review, once reviewed and approved it is then processes via required signature approval process which includes agency Secretary, Chief Information Officer, Chief Financial Officer, General Counsel, Taxation & Revenue, review by DoIT General Counsel and subsequent signature approval by Secretary and General Services Division Contract Review Bureau. Some IT contracts and amendments will not

require the DoIT Secretary's signature due to funding, but those are limited. Requests for Proposal require agencies to follow the General Services Department State Purchasing Division guidelines, and this also includes adding the approval process defined above process for contracts and amendments. Process for approvals related to IT purchases, especially contracts, amendments and RFP's take a significant amount of time due to signature or approval process. There are documented instances in which delays are introduced by changes in staff, reviews by entities, agencies and vendors, signature authority or availability of individuals with signature authority. Adding additional reviews and approvals, especially at a technology review process, will only add to this delay and duplicates review process.

**ADMINISTRATIVE IMPLICATIONS:** SB129 gives overall authority to Cybersecurity Office with no language to allow for an outside review or appeal process to orders issued by the office. Changes in procurement will cause unintentional and added delays to processing procurement documents.

**CONFLICT, DUPLICATION, COMPANIONSHIP, RELATIONSHIP:** Duplicates review process concerning contracts, contract amendments and requests for proposals by the Enterprise Project Mangement Office and General Services Department State Purchasing Office and Contracts Review Bureau.

The amended language of the bill looks to be expanding the oversight scope of the office without changing the definition of the term ""agency". The Cybersecurity office is an executive branch agency that does not seem to have jurisdiction over non-executive branch entities. This could potentially lead to legal battles when entities do not want to report to a body that has no jurisdiction over them.

**TECHNICAL ISSUES:** Appointment of designee by Security Officer to vote on issues related to compensation, discipline and supervision creates a conflict of interest for autonomy of advisory committee over the Cybersecurity Office and Security Officer. The Cybersecurity Office is attempting to provide guidelines and standards to entities it has no jurisdiction over.

**OTHER SUBSTANTIVE ISSUES:**

**ALTERNATIVES:**

**WHAT WILL BE THE CONSEQUENCES OF NOT ENACTING THIS BILL:** Cybersecurity will still be the responsibility of the Cybersecurity Office. Recommendations and policy creation will still take place. Security monitoring, detection, and remediation will continue. Responses to critical incidents will continue.

**AMENDMENTS:** Remove sections on approval of all information technology-related purchases. If specific examples or areas of concern are identified, list those. Remove the voting ability of the designee on matters related to discipline, compensation or supervision. Amend Section 3, paragraph D, replace "shall" with "may as best practice", this develops a better collaborative environment and the ability to open conversations on compliance of public entities, with State standards.