LFC Requester:	Austin Davidson

AGENCY BILL ANALYSIS
2024 REGULAR SESSION

WITHIN 24 HOURS OF BILL POSTING, UPLOAD ANALYSIS TO:

AgencyAnalysis.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 1/25/24
Bill No: Senate Bill 129

Sponsor: Michael Padilla
Debra Sariñana
Short Title: Amending the Cybersecurity Act

Agency Name and Code Number: Administrative Office of the Courts 218-00
Person Writing Cassandra Hayne
Phone: 505 819 8259 **Email** chayne@nmcourts.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	$100,000	$100,000	$200,000	Recurring	General Fund

(Parenthesis ( ) Indicate Expenditure Decreases)

SB129 would require the judiciary to track all information technology (IT) expenditures across an entire branch of government and provide this information to the cybersecurity office. Requests for proposals, contracts, contract amendments, and potential appropriation requests would all need to be identified, documented, reported to the cybersecurity office, and tracked for resolution. This is unworkable for multiple reasons, but at a minimum would require an additional FTE with IT experience to complete these duties.

Duplicates/Conflicts with/Companion to/Relates to:

Duplicates/Relates to Appropriation in the General Appropriation Act

SECTION III: NARRATIVE

BILL SUMMARY

Synopsis: SB 129 amends and significantly extends the reach and duties of the cybersecurity office.

The cybersecurity office was established in 2023 and is administratively attached to the Department of Information Technology (DoIT). The office is managed by the security officer and includes the creation of the statewide cybersecurity advisory committee.

This bill extends the reach and control of the cybersecurity office to all entities that receive general fund appropriations from the legislature, and establishes reporting and approval duties for IT expenditures, RFPs, contracts, contract amendments, and appropriation requests.

FISCAL IMPLICATIONS

SB129 adds significant tracking and reporting duties to the judicial branch and would require one additional FTE to complete these duties.

SIGNIFICANT ISSUES

The bill creates significant and inappropriate restrictions on the independence of the judicial branch of government and creates an unnecessary and duplicative review and approval processes for judicial branch IT and security expenditures and investments.

The bill would allow the cybersecurity office to monitor and audit judicial networks and systems, which infringes upon the independence of the judicial branch, is overly intrusive, and is entirely duplicative of our own efforts.

SB129 does not define what constitutes “cybersecurity expenditures” or “information security” in reference to contracts and appropriations.

Requiring “all information technology and cybersecurity expenditures” be reported to the cybersecurity office, as well as approval of all IT related RFPs, contracts, amendments and proposed appropriations is overly broad and significantly increases the workload of staff at all impacted entities, and it is not clear that the cybersecurity office has sufficient staff to perform a meaningful review of this information. The goal of such extensive involvement is also not clear.

SB129 does not define what constitutes “transacting business with the state” and it is not clear how rules would be enforced against private entities if not included in governing contractual language.

Given the very high sensitivity of state network and security data, it is imperative that all security testing, scans, analysis, audits, and related activities completed, managed, or required by the cybersecurity office be performed within the boundaries of the United States and by US-based entities and contractors.

PERFORMANCE IMPLICATIONS

ADMINISTRATIVE IMPLICATIONS

CONFLICT, DUPLICATION, COMPANIONSHIP, RELATIONSHIP

TECHNICAL ISSUES

OTHER SUBSTANTIVE ISSUES

SB129 defines and expands the duties of the cybersecurity office and security officer. Section 3, item D defines standards for public bodies not subject to the jurisdiction of the security officer. It is not clear that this is relevant to the bill or enforceable.

ALTERNATIVES

WHAT WILL BE THE CONSEQUENCES OF NOT ENACTING THIS BILL

There will be no significant consequences if SB129 is not enacted.

AMENDMENTS