LFC Requester:	Emily Hilla

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** X

Date 2/7/24
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	$150.00	$150.00	$300.00	Recurring	General Fund

(Parenthesis ( ) Indicate Expenditure Decreases)

SB129 would require the judiciary to track all cybersecurity information technology (IT) security expenditures across an entire branch of government and provide this information to the cybersecurity office. Cybersecurity expenditures in the Judiciary would need to be identified, documented, reported to the cybersecurity office, and tracked for resolution. These new administrative duties at a minimum would require an additional 1 to 1.5 senior FTE(s) with IT experience; these additional FTEs are in addition to existing Judiciary cybersecurity staff.

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 and the security officer.

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 to 1 1/2 additional FTE to complete these administrative duties.

SIGNIFICANT ISSUES

SB 129 implicates constitutional separation of powers issues. Section 3, Paragraph C of the bill uses ambiguous language to grant the security officer almost unlimited authority to control the judiciary's computer systems in the event of an undefined "imminent threat."

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

Additionally, the bill relies only on the authority of a single branch of government. The administrative rulemaking process does not ensure the needs of the judicial branch are understood or included.

Section 3, Paragraph (B)(1) requires all public bodies to report cybersecurity expenditures, but in a form, manner, and scope determined solely by an executive agency appointee. Then, Section 3, Paragraph (D) mandates public bodies report that they meet certain minimum cybersecurity standards, based on what the security officer deems adequate pursuant to their exclusive rulemaking. It also suggests that the security officer would then participate in a compliance assessment in the event of any concern; allowing access to judicial IT assets should not be established in statute.

The necessary and prudent goals described by these sections could be accomplished via other means, such as requiring coordination or contractual agreements between separate branches or bodies of government, rather than the present means of administrative rulemaking.

The bill contains ambiguous and contradictory language that could be interpreted to allow the cybersecurity office to monitor and assess judicial networks and systems, which infringes upon the independence of the judicial branch, is overly intrusive, and is entirely duplicative of our own efforts. AOC fully supports the intent of strong security standards, and currently complies with standards published by the national institute of standards and technology. However, the bill subjects the judicial branch to an executive branch certification process based on undefined compliance qualifications established by the executive branch, and further allows the executive branch to assess judicial compliance levels without sufficient knowledge of unique judicial needs and obligations.

Requiring “all information technology and cybersecurity expenditures” be reported to the cybersecurity office is 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.

Given the very high sensitivity of state network and security data, it is imperative that all security testing, scans, analysis, assessments, 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

Section 3 Paragraph B appears is inconsistent, as grants powers to the cybersecurity office over “agencies” but in the enumerated powers includes authority over “public bodies” which is specifically defined much more broadly than executive branch agencies.

Section 3 Paragraphs D and E are inconsistent and appear to be in conflict with one another. One paragraph establishes a requirement than the next paragraphs describes as voluntary. This language makes it difficult to clearly interpret the bill.

OTHER SUBSTANTIVE ISSUES

SB129 defines and expands the duties of the cybersecurity office and security officer. The original Act more clearly defined the authority of the security officer to specifically exclude non-executive agencies and other entities, including tribal governments. This language has been removed, resulting in potential separation of powers and tribal sovereignty issues.

ALTERNATIVES

WHAT WILL BE THE CONSEQUENCES OF NOT ENACTING THIS BILL

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

AMENDMENTS