LFC Requester:	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** ____

Date 2/7/24
Bill No: CS/CS/SB129

Sponsor: Padilla/Sariñana
Short Title: CYBER SECURITY ACT CHANGES

Agency Name and Code Number: OSA 308
Person Writing D. Craig
Phone: 505-699-9911 **Email** David.Craig@osa.nm.gov

SECTION II: FISCAL IMPACT

APPROPRIATION (dollars in thousands)

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

(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	Indeterm.	Indeterm.	Indeterm.	Indeterm	Recurring	GF

(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

The Senate Finance Committee substitute for the Senate Health and Public Affairs Committee substitute for Senate Bill 129 (CS/CS/SB129) amends the Cybersecurity Act ("the Act") to expand the powers and oversight responsibilities of the Cybersecurity Office (or "the office") within the Department of Information Technology (DoIT). CS/CS/SB129 clarifies definitions to include local public bodies. The bill expands rules making authority to include oversight of all entities receiving general fund appropriations and persons/entities transacting with the state and require any entity receiving general fund appropriations to report information technology (IT) and cybersecurity expenditures in a form and manner prescribed by DoIT. CS/CS/SB129 empowers DoIT to conduct IT and security assessments. CS/CS/SB129 clarifies rulemaking authority for various existing duties such as minimum classification, standards and design controls, cybersecurity awareness policies and training standards, and data breach processes. CS/CS/SB129 adds new authority to approve all IT requests for proposals (RFP's), cybersecurity and IT contracts and contract amendments (including emergency, sole source or price agreement procurements), and requires DoIT to review and make recommendations on agency, public school, higher education and county and municipality cybersecurity or information security projects prior to Legislative appropriation.

CS/CS/SB129 expands powers of the Security Officer within the Cybersecurity Office to issue orders regarding compliance of agencies with its rules, policies, standards, and controls issued by the office, and allows adoption to be optional by counties, municipalities, or tribal governments. CS/CS/SB129 does require those entities not subject to the jurisdiction of the office (such as counties, municipalities, or tribal governments) to adopt policies, standards and procedures based upon the national institute of standards and technology.

CS/CS/SB129 changes the role of the security office on the cybersecurity advisory committee from a non-voting member to a voting member but recuses them from discussions related to their performance and requires a non-DoIT employee to vote on those issues. CS/CS/SB129 adds the Department of Homeland Security to the advisory committee and allows the Governor to appoint two members of her choice, one each with experience in public education and public health cybersecurity.

CS/CS/SB129 does not contain an appropriation.

FISCAL IMPLICATIONS

CS/CS/SB129 would increase the volume of contracts, contract amendments, legislative requests and other cyber security appropriations or procurements by redirecting these requests or procurements from the user entity to DoIT. OSA does not have view access to SHARE Financials necessary to run or extrapolate cost volume estimates for state agencies that are procuring with cybersecurity vendors. Nor does OSA receive or have access to data on agency budget requests in such a granular form as to determine which agencies, local public bodies, institutes of higher education or other entities have legislative appropriation requests for cybersecurity greater than $25 million.

OSA also has not been given access to statewide email distribution lists by DoIT so we may email chief information officers to receive anecdotal information on fiscal impacts to their agencies. As such, we are unable to produce more quantitative fiscal impacts until such time as we are given access to the data that many state agencies appreciate.

It is assumed that some amount of costs will be assumed for DoIT in increase staff and workload but without data these amounts are indeterminate. Without an appropriation or offsetting amount in the Operating Budget proposals, the DoIT operating budget would need to subsume these costs.

SIGNIFICANT ISSUES

On page 4, line 19, CS/CS/SB129 expands the role of the cybersecurity office to include new duties to "conduct information technology and security assessments." This change from the word audit to assessment alleviates previous concerns OSA had with use of the term IT audit and its confliction with OSA's authority to conduct SOC audits (see "Other Substantive Issues" below for background) for which the OSA of the state auditor has begun implementation for the state. There are three different types of SOC Audits, SOC-1, SOC-2, and SOC-3, DoIT would not be qualified to perform either a SOC-1 or SOC-2 but may be certified to conduct at SOC-3 audit. The OSA is including definitions and qualifications for SOC Audits in its next revision of the Audit Rule. The OSA is vetting the review of audit firm profiles qualified to perform SOC audits (through peer review processes) and requiring the SHARE system to undertake a SOC-2 audit as it transfers to DFA to ensure the state's main enterprise resource planning (ERP) system is safeguarding its most important financial data. An audit requires independence for management controls, which DoIT would be unable to perform since it creates the internal control system for its system.

Additionally, the new section 15 beginning on page 6, line 20 requiring the review and recommendation of all agency, public school, higher education institution, county, and municipality legislative appropriation requests for communications and information technology projects that incorporate protection of personal, sensitive or confidential information prior to submission to the Legislature alleviates some of the previous OSA concerns regarding the Legislature abdicating its role in reviewing and approving IT appropriation requests to DoIT.

PERFORMANCE IMPLICATIONS
ADMINISTRATIVE IMPLICATIONS

CONFLICT, DUPLICATION, COMPANIONSHIP, RELATIONSHIP

TECHNICAL ISSUES

The phrase “experience in cybersecurity” is used as a qualification for various board members, however “experience in cybersecurity” is not defined and is ambiguous. It is suggested that a definition with minimum qualifications be defined for this term to achieve legislative intent.

OTHER SUBSTANTIVE ISSUES

In 2017, the American Institutes of Certified Public Accountants (AICPA) developed the term system and organization controls (SOC) to refer to the suite of services practitioners may provide relating to system-level controls of a service organization and system or entity-level controls of other organizations. SOC audits measure information system controls under five categories (security, availability, processing integrity, confidentiality, and privacy) called Trust Service Criteria. These five categories were created to directly correlate to the Committee of Sponsoring Organizations of the Treadway Commission (COSO) Internal Control - Integrated Framework (also known as “the COSO Framework for Internal Controls”) that all entities must use in conducting financial and other operations. They also may be directly mapped to the National Institute of Standards and Technology’s (NIAST’s) Special Publication 800-53 which documents acceptable information technology controls for most of the federal government outside of the Department of Defense.

ALTERNATIVES

WHAT WILL BE THE CONSEQUENCES OF NOT ENACTING THIS BILL

The cybersecurity office will maintain its current scope of powers and duties and will not be become a voting member of their oversight board.

AMENDMENTS