FISCAL IMPACT REPORT

SPONSOR SFC **LAST UPDATED** 2/14/24
ORIGINAL DATE 2/7/24
BILL NUMBER CS/CS/Senate Bill 129/SHPACS/SFCS/ aHJC

SHORT TITLE Cybersecurity Act Changes

ANALYST Hilla

ESTIMATED ADDITIONAL OPERATING BUDGET IMPACT*

(dollars in thousands)

Agency/Program	FY24	FY25	FY26	3 Year Total Cost	Recurring or Nonrecurring	Fund Affected
AOC		$100.0	$100.0	$200.0	Recurring	General Fund
OSI		$280.0	$280.0	$560.0	Recurring	General Fund
Council Per Diem		At least $12.1	At least $12.1	At least $24.2	Recurring	General Fund
Total		At least $392.1	At least $392.1	At least $784.2	Recurring	General Fund

Parentheses ( ) indicate expenditure decreases.
*Amounts reflect most recent analysis of this legislation.

Relates to an appropriation the General Appropriation Act of 2024 (HB2): $1.6 million for Cybersecurity Office expansion as well as $5.5 million for a Cybersecurity Special in Section 5.

Sources of Information

LFC Files
National Association of State Chief Information Security Officers (NASCIO)
Agency Analysis Received From
Administrative Office of the Court (AOC)
Department of Information Technology (DoIT)
Department of Finance and Administration (DFA)
Department of Homeland Security and Emergency management (DHSEM)
Indian Affairs Department (IAD)
Office of Broadband Access and Expansion (OBAE)
Office of State Auditor (OSA)
Office of Superintendent of Insurance (OSI)

Agency Analysis was Solicited but Not Received From
Office of the Governor
New Mexico Counties

SUMMARY

Synopsis of HJC Amendment to SFC Substitute for SHPAC Substitute for Senate Bill 129

The House Judiciary amendment to the Senate Finance Committee substitute for the Senate Health and Public Affairs Committee substitute for Senate Bill 129 changes the definition a public body to being defined as a county, municipality, public school or institution of higher education. The amendment. The amendment makes it so that public bodies that receive general fund appropriations used for information technology resources, regardless of jurisdiction of the security officer, shall adopt and implement cybersecurity, information security and privacy policies, standards and procedures issued by the national institute of standards and technology. A public body or another branch of government may voluntarily comply with the rules, standards, orders and other requirements of the Cybersecurity Act following the amendment.

Synopsis of SFC Substitute for SHPAC Substitute for Senate Bill 129

The Senate Finance Committee substitute for the Senate Health and Public Affairs Committee substitute for Senate Bill 129 amends the Cybersecurity Act for the following:

- Adds a definition for "public body" in the Cybersecurity Act; a "public body" means a branch, agency, department, institution, board, bureau, commission, district or committee of the state or a county, municipality, public school or institution of higher education.
- Adds requirement of certification of compliance of certain information security standards; the security officer may report any compliance concerns to authorized oversight entities and cooperate with any compliance assessment.
- Requires entities receiving general fund appropriations from the legislature to report all cybersecurity and information technology security expenditures to the Cybersecurity Office in a form and manner established by the Office;
- Requires the Office to adopt and implement rules establishing minimum cybersecurity controls for managing and protecting information technology assets and infrastructure for all entities that are connected to an agency-operated or -owned telecommunications network; adopt and implement rules to establish minimum data classification policies and standards; adopt and implement rules to develop and issue cybersecurity awareness policies; adopt and implement rules to establish a centralized cybersecurity and data breach reporting process;
- Requires the Office to approve agency cybersecurity and information security requests for proposals and invitations for bids that are subject to the Procurement Code;
- Requires the Office to review and approve all agency, public school, higher education institution, county and municipality legislative appropriation requests related to cybersecurity and information security projects that incorporate protection of personal, sensitive, or confidential information as defined by the Office prior to submission of such request to the legislature; and
- Public bodies not subject to the jurisdiction of the security officer may voluntarily adopt and implement cybersecurity, information security and privacy policies, standards and procedures based upon minimum standards issued by the national institute of standards and technology. A public body shall certify compliance with the applicable standard during the preceding fiscal year.

This bill does not contain an effective date and, as a result, would go into effect 90 days after the Legislature adjourns, or May 15, 2024, if enacted.

FISCAL IMPLICATIONS

The bill does not contain an appropriation. Public members of the new cybersecurity advisory council or subgroup established by the bill may receive per-diem and mileage reimbursement in accordance with Sections 10-8-1 through 10-8-8 NMSA 1978 (the Per Diem and Mileage Act). Mileage costs would vary widely and are difficult to estimate. However, based on the rate of $155 per day for the 13 members, per diem would have a minimal fiscal impact, likely less than $20 thousand annually. Assuming one meeting every other month, the total estimated per diem costs to operate the council would be $12.1 thousand.

The Administrative Office of the Court (AOC) states that the bill would require judiciary tracking of all information technology (IT) expenditures across an entire branch of government and provide this information to the Cybersecurity Office. AOC says this would require at least one additional FTE for an IT position to help manage the identification, documentation, and reporting to the Cybersecurity Office for requests for proposals, contracts, contract amendments, and potential appropriation requests.

As outlined in the bill, security audits will be conducted, but there is no specification of how much these audits will cost and who will be paying for these audits. The Department of Finance and Administration (DFA) says that the Cybersecurity Office should consider providing grants to entities to cover the increased cost of implementing rules covered in the bill, which would be done by adding a baseline to all IT appropriations to cover these costs. According to OSA, the office currently conducts information technology and security audits.

The Office of Superintendent of Insurance states that the annual fiscal impact on the agency would be around approximately $280 thousand each fiscal year to over 2 FTE and a one new subscription to a log collection software.

The General Appropriation Act of 2024 (CS/HB 2&3) contains an appropriation of $1.6 million for the Cybersecurity Office's expansions. This bill would increase the Office's duties, which was addressed in the Department of Information Technology's (DoIT) initial agency request. HB 2 also contains a $5.5 million special for cybersecurity initiatives including public and higher education.

SIGNIFICANT ISSUES

At least 18 states have a cybersecurity strategic plan in place, according to the National Association of State Chief Information Officers (NASCIO). The bill notes the advisory committee shall assist in the development of a state cybersecurity plan but does not provide descriptions or requirements for what should be included in that plan. According to federal guidance, a cybersecurity plan should include detailed, actionable plans for identifying, protecting, detecting, responding to and recovering from cyber incidents. The plan should include things like a spending plan, an asset inventory, and an overview of the state's detection or recovery processes to be implemented in the case of a cybersecurity incident.

Although some of New Mexico's cybersecurity operations and policies are housed within DoIT, state cyber operations are siloed in different agencies, which is significantly more expensive and difficult to maintain compared to alternative structures. In 2018, only two states still operated a decentralized system while 15 states were operating a hybrid structure, which offers more flexibility and economies of scale while allowing individual agencies to retain some level of purchasing power. To strengthen governance, many states have mandated or created cybersecurity advisory councils, which would be accomplished in New Mexico through this bill.

DoIT says that clarifying the rules establishing minimum security standards and policies are applicable to entities receiving general fund appropriations is necessary to fully defend and protect the state's IT infrastructure from cybersecurity attacks and related information security incidents. Without implementation of security standards, some entities in the state can be left vulnerable, which could impact all entities on that infrastructure. Allowing the issuing of compliance rules allows for accountability with federal, state, and the cybersecurity office's guidelines and standards. The modification of 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.

There are multiple kinds of audits for information technology called system and organization controls (SOC) audit. There is a SOC-1, SOC-2, and SOC-3 audit. DoIT could potentially do a SOC-3 audit but is not qualified to perform the other kinds of SOC audits. OSA says that "an audit requires independence for management controls, which DoIT would be unable to perform since it creates the internal control system for its system. SB129 conflicts with this work and repositions the role of state oversight of SOC audits to DoIT. If SB129 were to pass, the OSA would no longer have the authority to request an SOC audit for any state agency, including the ongoing request for the SOC audit of DFA and DoIT. OSA does not support the repositioning of SOC audit firm approval and determining conditions by which SOC audits are required of state agencies from the independent OSA to an Executive branch agency overseeing other Executive branch agencies." The change of language in the SFC substitute changing "audit" to "security assessments" alleviates these concerns previously stated by OSA.

OSA further adds that "Article III, Section 1 of the New Mexico Constitution regarding separation of powers has generally been construed that the Legislature cannot delegate the power to appropriate to another branch of government unless specifically authorized to due so by the State Constitution (see State ex rel. Schwartz v. Johnson, 1995-NMSC-080, 120 N.M. 820, 907 P.2d 1001). It is unclear if the Legislature requiring an Executive Branch agency to review and approve county and municipality cybersecurity legislative appropriation requests prior to submission to the legislature would meet the test of delegation of appropriation power."

AOC says that 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 process 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." The amendment of the definition of "public body" addresses some of AOC's concerns as the agency, alongside other judicial agencies, can voluntarily comply with the rules and requirements of the Cybersecurity Act and are not confined to do so as with the previous definition of "public body."

The Department of Public Safety states that although not included in the bill, the representation of law enforcement on the committee would be beneficial as the FBI designated Criminal Justice Information Services (CJIS) Information Security Officer undergoes training by the FBI on best cybersecurity practices and policies. DPS states that the omission of the CJIS Information Security Officer is a lost opportunity.

PERFORMANCE IMPLICATIONS

DFA states that purchases and contracts within the Cybersecurity Office require approval by both DoIT and DFA. Any contracts or amendments related to IT purchases are reviewed by DoIT's Enterprise Project Management Office (EMPO). Contingent upon funding and any additional requirements set by EMPO, DFA says then the "contracts 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

DFA says that the bill does not allow for an outside review or appeal process to orders, and changes in procurement will cause unintentional and add delayed to processing procurement documents.

CONFLICT, DUPLICATION, COMPANIONSHIP, RELATIONSHIP

DFA states the bill "duplicates review process concerning contracts, contract amendments and requests for proposals by the Enterprise Project Management 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."

Relates to appropriations in the General Appropriation Act of 2024 (HB2).

TECHNICAL ISSUES

AOC adds that the bill does not define what constitutes "cybersecurity expenditures."

OSA adds:

> 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.

EH/rl/cf/al/ne/ss