LEGISLATIVE EDUCATION STUDY COMMITTEE
BILL ANALYSIS
56th Legislature, 2nd Session, 2024

Bill Number SB129/SHPACS/SFCS **Sponsor** Padilla/Sariñana

Tracking Number .228048.1 **Committee Referrals** SCC/SHPAC/SFC

Short Title Cybersecurity Act Changes

Analyst Bedeaux **Original Date** 1/29/2024
Last Updated 2/7/2024

BILL SUMMARY

Synopsis of Bill

The Senate Finance Committee Substitute for the Senate Health and Public Affairs Committee Substitute for Senate Bill 129 (SB129/SHPACS/SFCS) makes a number of changes to the Cybersecurity Act (Chapter 9, Article 27A, NMSA 1978) to accomplish the following:

- Define "public body" in the Cybersecurity Act to include 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.

- Ensure the minimum security standards adopted by the Cybersecurity Office, an administrative arm of the Department of Information Technology (DoIT), are applicable to all public bodies receiving general fund appropriations.

- Give the Cybersecurity Office authority over information technology and security audits.

- Require all public bodies receiving general fund appropriations from the Legislature to report to the Cybersecurity Office all information technology and cybersecurity expenditures in a form and manner of the office's choosing.

- Require public bodies outside the jurisdiction of the security officer – including non-executive-cabinet state agencies, school districts, charter schools, and institutions of higher education – to adopt and implement cybersecurity, information security and privacy policies, standards, and procedures based upon no less than moderate-impact security control baselines issued by the national institute of standards and technology National Institute of Standards and Technology (NIST).

- Gives the Cybersecurity Office authority to establish a form and manner for public bodies outside the jurisdiction of the security officer to report their cybersecurity, information security, and privacy policies. The security officer may report any compliance concerns to authorized oversight entities.

- Give the Cybersecurity Office authority to review requests for proposals (RFPs) for information technology projects and security contracts and amendments prior to their approval.

- Give the Cybersecurity Office authority to review all agency, public school, higher education institution, county, and municipality requests for appropriations related to cybersecurity and information security that incorporate protection of personal, sensitive, or confidential information.

- Give the state security officer authority to issue orders to ensure agencies' compliance with rules and recommendations of the Cybersecurity Office or as necessary to protect the state's digital assets from imminent threats.

Other public bodies outside the jurisdiction of the security officer are required to implement cybersecurity policies based on the minimum standards issued by the National Institute of Standards and Technology.

SB129/SHPACS/SFCS amends the membership of the Cybersecurity Advisory Committee as outlined in 9-27A-5 NMSA 1978. The bill establishes the state cybersecurity officer as a voting member of the committee, provided that the officer must be replaced by an alternate person who is not an employee of the Cybersecurity Office for matters related to supervision, discipline, or compensation of the security officer. SB129/SHPACS/SFCS adds the secretary of Homeland Security and Emergency Management or the secretary's designee to the committee. The bill also provides that two members shall be appointed by the governor, one who has experience with cybersecurity issues for public education and another for public health.

FISCAL IMPACT

SB129/SHPACS/SFCS does not contain an appropriation.

The bill substantially increases the duties and powers of the state Cybersecurity Office to perform audits, monitor executive cabinet agencies' compliance with rules and regulations, and review proposed cybersecurity projects that involve general fund dollars. Analysis from DoIT notes the agency may need additional FTE to oversee the new duties. To support the expansion of the Cybersecurity Office's duties, the House Appropriations and Finance Committee Substitute for House Bills 2 and 3 as amended by the House (HB2/HAFCS/aHFl#1) includes an appropriation of $6.3 million for the Cybersecurity Office, an increase of $1.6 million from FY24 recommended in the Legislative Finance Committee (LFC) budget framework for FY25.

SB129/SHPACS/SFCS requires all public bodies that receive general fund appropriations for information technology resources to adopt and implement cybersecurity, information security, and privacy policies, standards, and procedures based on moderate-impact security control baselines adopted by NIST. As such, the bill would require all public schools and institutions of higher education comply with new administrative requirements, potentially resulting in new costs for public schools. Depending on the status of school district and charter schools' cybersecurity infrastructure, schools may need additional funds to reach a level of compliance with NIST standards. The extent of the new funding required is difficult to estimate and depends entirely on individual schools' level of compliance.

SUBSTANTIVE ISSUES

The Cybersecurity Office, established by Laws 2023, Chapter 115 (Senate Bill 280), has been in operation for one year. During that year, the office published a Statewide Cybersecurity Plan, structured around four primary goals for the agency:

1. Manage and monitor information systems, data, and networks.
2. Enhance cybersecurity resilience.
3. Develop statewide cybersecurity and risk management strategies.
4. Train and develop the cybersecurity workforce.

Within each goal, the office lists several actionable objectives and performance metrics to monitor the state's progress toward meeting the goal. The plan offers the state a strong, actionable roadmap to improved cybersecurity, but does not provide any direct legislative recommendations or request funding for particular priorities. SB129/SHPACS/SFCS is a state agency bill, likely structured to give the Cybersecurity Office additional authority to meet its strategic goals.

Subsection B of Section 9-27A-3 NMSA 1978 gives the Cybersecurity Office jurisdiction over executive cabinet agencies and their administratively attached agencies, offices, boards and commissions. Executive cabinet agencies are required comply with administrative rules adopted by the Cybersecurity Office, which govern a variety of topics, including the following:

- Access control;
- Applications;
- Wireless and wired networks;
- Remote access;
- Bluetooth;
- Radio frequencies;
- User registration and password management;
- Personal devices;
- Scanning for vulnerabilities;
- Intrusion testing;
- Telephones and fax equipment;
- Modem usage; and
- Log-on banners.

SB129/SHPACS/SFCS notes that public bodies – defined to include school districts, charter schools, and institutions of higher education – may voluntarily follow the administrative rules adopted by the Cybersecurity Office.

SB129/SHPACS/SFCS would also require public bodies that receive general fund appropriations for information technology projects to implement cybersecurity policies based on NIST moderate-impact security control baselines. NIST is an administrative arm of the U.S. Department of Commerce which uses rigorous scientific research to develop standards for science and technology equipment nationwide. The NIST standards range from low-impact to high-impact; the moderate-impact security control baseline includes 287 individual standards. It is unclear how the Cybersecurity Office will choose to monitor public bodies' implementation of the standards, but verifying the presence of each of the 287 standards for all public school technology projects may be a significant undertaking, potentially increasing the time and costs associated with each project.

Cybersecurity has been a challenge for many New Mexico school districts, which have become the targets of cyber-attacks in recent years. Hackers typically attempt to extort schools for money, stall school operations, and steal sensitive student information. Many small, rural New Mexico school districts do not have the resources, manpower, or expertise to fully manage their cybersecurity needs, and may need to rely on outside help to ensure their networks and systems are secure. The statewide Cybersecurity Office could benefit many schools by providing centralized expertise to oversee their cybersecurity practices. However, the oversight to public schools should be accompanied by additional resources to ensure schools are able to comply with the Cybersecurity Office's regulations.

ADMINISTRATIVE IMPLICATIONS

Analysis from the Office of the State Auditor (OSA) notes that OSA already performs "system organization and controls" audits for state agencies. OSA explains the bill would conflict with current processes, repositioning the role of cybersecurity audits from OSA to the Cybersecurity Office.

SB129/SHPACS/SFCS gives the Cybersecurity Office authority to approve RFPs for IT projects prior to their approval. Under SB129, any school district or charter school that issues an RFP for an IT project would be required to submit the proposals received to the Cybersecurity Office; schools would not be allowed to proceed with any project proposals found to violate the office's regulations. The new RFP approval process may result in a large amount of administrative work for the Cybersecurity Office, and depending on the office's staffing levels, may significantly slow down the ability of schools to spend IT funds.

Similarly, SB129/SHPACS/SFCS would require any agency requesting more than $25 million for an IT project to undergo a review by the Cybersecurity Office. This process would likely mirror the current process for many state agency web applications. Currently, state agencies seeking funding for IT projects work with the DoIT Enterprise Project Management Office to ensure appropriations support viable, well-thought-out IT projects. The Cybersecurity Office's compliance check may be integrated into the current DoIT approval process, but may create additional administrative barriers to funding for IT projects.

TECHNICAL ISSUES

Analysis from OSA points out that removing the power of appropriation from the Legislature violates Article III, Section 1 of the New Mexico Constitution, which states the Legislature cannot delegate the power to appropriate to another branch of government.

RELATED BILLS

Related to SB45, Broadband Infrastructure, which transfers the education technology infrastructure deficiencies correction program from the Public School Facilities Authority to the Office of Broadband Access and Expansion.

SOURCES OF INFORMATION

- LESC Files
- Office of Broadband Access and Expansion (OBAE)
- Office of the State Auditor (OSA)

- Department of Homeland Security and Emergency Management (DHSEM)
- Department of Finance and Administration (DFA)
- Office of the Superintendent of Insurance (OSI)
- Department of Information Technology (DoIT)
- Administrative Office of the Courts (AOC)
- Indian Affairs Department (IAD)

TB/mca/js