LEGISLATIVE EDUCATION STUDY COMMITTEE
BILL ANALYSIS
57th Legislature, 1st Session, 2025

Bill Number SB254/SRCS **Sponsor** SRC

Tracking Number .231078.2 **Committee Referrals** SRC/SHPAC

Short Title Cybersecurity Act & Office Changes

Analyst Montoya **Original Date** 2/15/2025
Last Updated 3/7/2025

BILL SUMMARY

Synopsis of Bill

The Senate Rules Committee Substitute for Senate Bill 254 (SB254/SRCS) would amend the Cybersecurity Act (Section 9-27A-1 NMSA 1978) by renaming an existing office, making changes to the membership of an existing advisory committee, and clarifying the role of the officer that leads the current Cybersecurity Office. Changes in SB254/SRCS begin with modifying the title of the "Cybersecurity Office" to the "Office of Cybersecurity" throughout the Cybersecurity Act. The current Cybersecurity Office is created and administratively attached to the Department of Information Technology (DoIT), which SB254/SRCS retains.

SB254/SRCS would define "state-operated or state-owned telecommunication network" as a telecommunications network controlled by DoIT pursuant to the to the Department of Information Technology Act. SB254/SRCS would also clarify the proposed Office of Cybersecurity's role in overseeing the development of minimum cybersecurity controls for information technology assets and infrastructure. SB254/SRCS specifies that these controls apply to all entities connected to a "state-operated or state-owned" network, instead of applying to "agency-operated or -owned" telecommunications networks, as currently stated in law.

SB254/SRCS would expand the required minimum security standards and policies established by the Office to include a focus on "confidentiality" and secure "transmission" of information.

SB254/SRCS would grant the security officer, a position appointed by an existing Cybersecurity Advisory Committee, voting rights within that committee, although they would be required to be recused from deliberations and votes concerning supervision, discipline or compensation of the security officer. The security officer currently has a non-voting advisory role and oversees the existing Cybersecurity Office. Under SB254/SRCS, the security officer would continue to oversee the Office of Cybersecurity.

SB254/SRCS would change the Administrative Office of the Courts membership to one member appointed by the Chief Justice of the Supreme Court who is experienced with cybersecurity issues.

SB254/SRCS would reduce the number of advisory board members appointed by the New Mexico Association of Counties and the New Mexico Municipal League so that each organization has two appointees apiece, instead of three. Additionally, the bill would increase the number of members appointed by the governor from three to four. The bill requires the selection of governor appointed members be in consultation with the state chief information officer with the goal of enabling the Cybersecurity Advisory Committee to satisfy any federal or state cybersecurity grant funding requirements.

FISCAL IMPACT

SB254/SRCS does not contain an appropriation.

SUBSTANTIVE ISSUES

National Cybersecurity Trends in Kindergarten through 12th Grade Schools. According to K12 SIX, a nonprofit organization focused on enhancing cybersecurity for kindergarten through 12th grade (K-12) schools in the United States, over the past decade, K-12 schools in the U.S. have faced a growing number of cyberattacks, with over 1,600 publicly reported incidents between 2016 and 2022. According to the U.S. Cybersecurity and Infrastructure Security Agency, since the Covid-19 pandemic, the increased adoption of advanced networking technologies in K-12 schools has improved efficiency but has also heightened cybersecurity risks. Cyberthreats have included ransomware attacks, where hackers encrypt school data and demand payment, as well as data breaches that expose sensitive student and staff information. Phishing scams have also been widespread, deceiving school personnel into divulging confidential data, as well as distributed denial-of-service (DDoS) attacks, which can prevent access to school information technology (IT) infrastructure and data from staff and students. These cyberattacks can disable school systems and disrupt learning. The trend has continued in recent years, with at least 120 school districts across the nation hit by major cyber incidents in 2023 alone. According to the U.S. Department of Education, school districts across the nation experience a cyberattack an average of five times a week. Given the increasing reliance on digital education tools and technology for day-to-day school operations, cybersecurity is a critical challenge for K-12 institutions.

Impact on New Mexico Schools. Over the past few years, several New Mexico school districts have been targeted by cyberattacks, highlighting the growing cybersecurity risks faced by educational institutions. In January 2022, Albuquerque Public Schools experienced a ransomware attack resulting in a two-day closure and disrupted access to student information systems, though no personal data was reported as compromised. According to Las Cruces Sun News, in 2019 and 2020 Las Cruces Public Schools and Gadsden Independent School District (GISD) also fell victim to respective cyberattacks that caused district-wide shutdowns of internet and communication systems. GISD was targeted twice in 2020. In 2022, Fort Sumner Municipal Schools suffered a cyberattack that may have resulted in access to sensitive data on students, staff, and parents. These incidents draw attention to the importance of cybersecurity measures in New Mexico's schools. While not exhaustive, these cases serve as examples of the types of attacks that have occurred in the state's public schools.

Ensuring Education Representation. Given the scale and importance of New Mexico's public education system, ensuring its representation on the council would be beneficial. While education appears to be one of several options for the governor's appointees proposed by SB254/SRCS, it is valuable to recognize it as a foundational perspective within the committee. With 89 school districts and 99 charter schools that serve about 311 thousand students, the education system plays

a vital role in the state. As cybersecurity becomes increasingly critical to protecting student data, securing digital infrastructure, and supporting uninterrupted learning, having a dedicated voice from the education community could strengthen the council's ability to address these evolving challenges effectively.

Efforts to Improve Connectivity and Cybersecurity. During the 2024 interim, LESC staff provided an update on New Mexico's Statewide Education Network (SEN) and the broadband landscape for education in the state. During the presentation, staff highlighted the SEN's role in improving broadband access and cybersecurity for New Mexico schools. The SEN connects K-12 schools to secure, high-capacity internet through existing infrastructure provided by Internet Service Providers (ISPs).

Schools can benefit from this network by gaining reliable, high-speed internet, cybersecurity monitoring, DDoS mitigation, and technical support, addressing challenges faced by districts with limited resources and staff to maintain secure communication networks. The Broadband Development and Connectivity Program (BDCP) is responsible for supporting the SEN's implementation and ongoing maintenance. BDCP falls under the auspices of the Department of Information Technology's Office of Broadband Access and Expansion (OBAE). It is funded by both federal and state sources, including the public school capital outlay fund, which is administered by the Public School Facilities Authority (PSFA).

OTHER SIGNIFICANT ISSUES

Office of Cybersecurity Oversight. The language in SB254/SRCS offering clarification to the Office of Cybersecurity's oversight of all entities that are connected to a state-operated or state-owned telecommunications network may include all IT infrastructure managed by non-executive agencies and state government-affiliated entities, rather than being limited solely to executive branch agencies. However, this consolidated oversight may be negated by language included in the Cybersecurity Act (Section 9-27A-5 NMSA 1978) which states "Pursuant to the Cybersecurity Act or other statutory authority, the security officer may issue orders regarding the compliance of agencies with guidelines or recommendations of the cybersecurity advisory committee; however, *compliance with those guidelines or recommendations by non-executive agencies or county, municipal or tribal governments shall be strictly voluntary*."

ADMINISTRATIVE IMPLICATIONS

Administrative implications of SB254/SRCS for affected agencies do not appear to be significant.

RELATED BILLS

Relates to Senate Bill 401, Broadband for Education, which would amend the Severance Tax Bonding Act to provide bonding for education technology infrastructure and create the education technology fund. It would also transfer the BDCP, which oversees the SEN, from the PSFA to OBAE.

SOURCES OF INFORMATION

- LESC Files
- Administrative Office of the Courts (AOC)
- Department of Health (DOH)
- Department of Information Technology (DoIT)

- Department of Public Safety (DPS)
- Health Care Authority (HAC)
- Office of Broadband Access and Expansion (OBAE)
- New Mexico Department of Justice (NMDOJ)

MAM/clh/mca/jkh