LEGISLATIVE EDUCATION STUDY COMMITTEE
BILL ANALYSIS
54th Legislature, 2nd Session, 2020

Bill Number SJM7 **Sponsor** Padilla

Tracking Number .216534.1 **Committee Referrals** SRC/SEC; HEC

Short Title Study School Cybersecurity Issues

Analyst Andrews/Bedeaux **Original Date** 2/3/2020
Last Updated 2/14/2020

BILL SUMMARY

Synopsis of Joint Memorial

Senate Joint Memorial 7 (SJM7) requests LESC to convene a task force to study cybersecurity issues threatening public schools. SJM7 requests that the education cybersecurity task force report its findings, conclusions, and recommendations to the governor and the Legislature by October 1, 2020.

FISCAL IMPACT

Legislative memorials do not carry appropriations.

SUBSTANTIVE ISSUES

Cyberattacks are a serious and consistent threat to public schools. A survey published last year by the National School Boards Association found that school officials are less prepared for cyberattacks than their peers in private sector companies. Security benchmarking organization Security Scorecard Inc. ranked public education last out of 17 industries in terms of overall cybersecurity practices. Over the past decade, hackers have developed sophisticated methods of capturing personal information, which poses a challenge to public schools that struggle to keep up with technological developments. In response to nationwide attacks, the Wall Street Journal reports 23 states have established cybersecurity commissions.

Malicious cyber activities are conducted for a variety of reasons, including financial gain, information theft, intellectual property theft, activist causes, to disable computer systems, and to disrupt the critical infrastructure of a government or organization. Commonly, hackers distribute "ransomware" on public computers, designed to lock a computer's core functions until the victim or the organization meets the hackers' demands. Cybersecurity issues are exacerbated by a workforce that is often not trained in first-line defenses against cybersecurity, which include avoiding suspicious links and not opening suspicious emails. As the Public Schools Facilities Authority (PSFA) notes in their analysis, cybersecurity is a multilayer effort that involves governance, policies, infrastructure, specialized personnel and services.

Across New Mexico, schools are facing issues with ransomware and other issues related to phone systems, entry access, and security cameras – all items that are connected to the Internet. The Federal Communication Commission's (FCC's) E-rate program provides funding for Internet infrastructure, but only provides basic funding for firewalls, which is often insufficient to meet the totality of school district's cybersecurity needs. Advanced cybersecurity features are currently not eligible for E-rate funding; however, cybersecurity is an active national conversation and several states, including New Mexico, have requested the FCC allow E-rate to fund cybersecurity programs. While the Public School Capital Outlay Council (PSCOC) makes annual awards to improve school building and security systems, it's unclear whether cybersecurity infrastructure would be covered under the awards program.

During the 2019 interim, cybersecurity issues threatening public schools were discussed in several statewide committees and councils. In January 2020, the K-12 Information Technology Directors Cybersecurity Workgroup presented its strategic plan to PSCOC. The report identifies essential and achievable goals to enable and empower New Mexico public schools to improve their unique systems. The strategic plan assumes the task force in SJM7 will be created, and anticipates the state will use the task force to synchronize and coordinate strategic cybersecurity initiatives. According to the report, the task force will not replicate existing programmatic or budgetary mechanisms, or interfere with previously defined cybersecurity roles; rather, it will provide a single platform to integrate public school cybersecurity initiatives, manage strategic policy and planning, and streamline cybersecurity governance structures.

ADMINISTRATIVE IMPLICATIONS

SJM7 requests LESC convene a seven-member education cybersecurity task force consisting of four representatives from school districts, the secretary of the Department of Information Technology (DoIT) or the secretary's designee, one representative from the Public Education Department, and one representative from PSFA.

RELATED BILLS

Relates to SJM9, Blockchain Technology Task Force, which requests DoIT to convene a blockchain technology task force to examine and report the potential benefits and risks to the public associated with the use of blockchain technology.

SOURCES OF INFORMATION

- LESC Files
- Department of Information Technology (DoIT)
- Public School Facilities Authority (PSFA)

MCA/TB/mc/sgs