F I S C A L I M P A C T R E P O R T

SPONSOR HEC **ORIGINAL DATE** 2/9/22 **LAST UPDATED** **HB** 122/HECS

SHORT TITLE School Cybersecurity Program **SB**

ANALYST Armatage/Liu

APPROPRIATION (dollars in thousands)

Appropriation					Recurring or Nonrecurring	Fund Affected
FY23	FY24	FY25	FY26	4 Year Total Cost		
$8,000.0	$10,000.0	$12,000.0	$15,000.0	$45,000.0	Recurring	General Fund

(Parenthesis ( ) Indicate Expenditure Decreases)

Relates to SB98
Relates to Appropriation in the General Appropriation Act

SOURCES OF INFORMATION
LFC Files

Other Responses
National Conference of State Legislatures (NCSL)

SUMMARY

Synopsis of Bill

The House Education Committee Substitute for House Bill 122 appropriates $45 million from the general fund to the Department of Information Technology (DoIT) between FY23 and FY26 to hire 3 FTE who will develop a cybersecurity program that meets federal standards for public schools, state special schools, and the statewide education technology infrastructure network. There is no effective date of this bill. It is assumed the effective date is 90 days following adjournment of the Legislature.

FISCAL IMPLICATIONS

The appropriation of $45 million contained in this bill is a recurring expense to the general fund. Any unexpended or unencumbered balance remaining at the end of FY26 shall revert to the general fund. Although the bill does not specify appropriations beyond FY26, establishing a new grant program could create an expectation the program will continue in future fiscal years; therefore, this cost is scored as recurring.

The bill phases funding over time for a cybersecurity programs that includes cybersecurity insurance support, planning and project management, development of a response and recovery plan and quarterly reviews, hardening of cyber-environment infrastructure, operations, processes and systems, monitoring network activity, and training for employees and students. The funding is awarded as such:

- $8 million in FY23 for at least 35 districts and 18 charters or special schools,
- $10 million in FY24 for at least 55 districts and 18 charters or special schools,
- $12 million in FY25 for at least 70 districts and 18 charters or special schools, and
- $15 million in FY26 for all district, charters, and special schools.

SIGNIFICANT ISSUES

Cyber attacks targeting school districts have increased both nationally and locally, including recent ransomware attacks on school districts in Albuquerque, Bernalillo, Gadsden, Las Cruces and Truth or Consequences. Cyber attacks can cause significant disruptions to the education of students and threaten the privacy of sensitive student and staff data.

Since 2018, New Mexico state and local government, hospitals, public school districts, and higher education institutions have been victim to at least 28 cybersecurity and ransomware attacks. In response, New Mexico appropriated $7 million to prevent cyber-attacks and manage associated risks. However, most of those dollars have supported planning and pilot-type activities, with very few widespread protections for state government.

New Mexico does not have a number of protections in place deemed best practice by other states or national organizations, including processes for reporting cyber incidents, and mandatory training for employees. For example, the state does not have a uniform cybersecurity process for reporting cyber incidents, or for entities seeking assistance.

In recognizing they had a fragmented cybersecurity system, the Iowa Information Security Division began offering cybersecurity awareness training for county and city governments, schools and hospitals, and worked with the Secretary of State's Office to enhance cybersecurity resilience of election infrastructure. Additionally, cybersecurity awareness training is a best practice to help employees protect themselves and their employer against cyber-attacks and threats. This type of training empowers employees with up-to-date knowledge on how to recognize and mitigate a cyber-threat.

New Mexico does not require state agency employees to participate in cybersecurity training. According to NCSL reports, every state offers cybersecurity training for state employees but only 16 states mandate training for employees. Texas and Oregon require annual cybersecurity training to occur on an agency-by-agency basis, and all state agencies must submit a cybersecurity plan annually.

The federal State and Local Cybersecurity Improvement Act (H.R.3138) created the State and Local Cybersecurity Grant Program to award grants "… to eligible entities [States or Indian tribes] to address cybersecurity risks and cybersecurity threats to information systems of State, local, or Tribal organizations (Section 2220A)." The grant program provides $1 billion dollars over four years to be administered by the Federal Emergency Management Agency. States must submit a Cybersecurity Plan for approval. Provisions of this bill would require DoIT to develop and implement a cybersecurity program that meets the standards of the federal act.

PERFORMANCE IMPLICATIONS

In 2018, the Legislature appropriated $1 million to DoIT to perform a statewide cybersecurity assessment to identify and implement security-related tools for compliance monitoring and cybersecurity risk management. In June 2019, DoIT announced a pilot project to provide quarterly vulnerability scans to agency chief information officers. The pilot was intended to help IT staff prioritize security risks, assign remediation tasks, and measure progress. At a cost of $593.9 thousand, DoIT contracted with RiskSense, an IT security expert that supports several state organizations, to perform quarterly vulnerability scans.

Through the pilot, RiskSense performed vulnerability scans on state assets for 42 executive agencies and three non-executive agencies (as of August 2020). The resulting data was loaded into the RiskSense platform – a tool to support analysis and remediation – and shared with DoIT. Although DoIT plans to use the information for cybersecurity-related trend analysis, it is not clear how DoIT communicates the results to participating state agencies, and what type of remediation activities are underway. RiskSense cybersecurity vulnerability scans occurred during the fourth quarter of FY20, and DoIT reported that as of November 2020, RiskSense on boarded 43 of 67 agencies (64.2 percent).

The vulnerability scans have a scoring system, and utilize a color-coded indicator of red, yellow and green, with green indicating less vulnerability and red indicating highly vulnerable. The score represents the organization's cybersecurity posture, measuring risk posed by vulnerabilities and identifies potential threats. According to DoIT, the RiskSense, Inc. tool and portal for reporting is consistently tuned, and the effectiveness of the reports have improved within one year of the pilot rollout.

ADMINISTRATIVE IMPLICATIONS

The statewide education network (SEN) referenced in the bill is also referenced in Section 22-24-4.5 NMSA 1978. Statute requires the Public School Capital Outlay Council (PSCOC), with the advice of DoIT, to develop guidelines for the SEN. PSCOC is also given the authority to approve allocations for the construction of the network. Statute does not delegate responsibility for, nor oversight of, the SEN. The Public School Facilities Authority (PSFA) recommends delegating the guidelines and funding of the SEN to PSCOC and keeping cybersecurity funding with education agencies or the Broadband Office under DoIT.

DoIT considers cybersecurity to fall under its direct oversight. The department has the necessary expertise in planning, design, project management, implementation and administration of cybersecurity initiatives to fulfill this role. Furthermore, DoIT highlights the existing shortage of cybersecurity professionals and difficulty state governments face in recruiting and retaining these personnel. The implementation of a comprehensive public sector cybersecurity initiative would be more effective and efficient than siloed programs.

RELATIONSHIP

This bill relates to Senate Bill 98, which creates a cybersecurity office at DoIT. The bill also relates to several appropriations in the HAFC Substitute for HB2, which includes $1 million to DoIT, $1.5 million to PED, $1.7 million to higher education institutions, and $990 thousand to the Department of Public Safety for cybersecurity.

OTHER SUBSTANTIVE ISSUES

In the context of growing cybersecurity risks exacerbated by a move to remote work and learning, states have devoted increased attention to the issue of cybersecurity. This year nine states have pending legislation related to cybersecurity in schools (NCSL). States have taken a range of approaches to educational cybersecurity. North Dakota authorized a statewide approach to cybersecurity strategy across all aspects of state government, including K-12 education (SB 2110). California authorizes the military department to consult with the California Cybersecurity Integration Center, at the request of a local educational agency (LEA), to perform an independent security assessment of the LEA or an individual school site (CA A 1352). Tennessee requires a state-level safety team to create a template safety plan that includes cybersecurity policies and procedures that LEAs must adopt (TN H 925).

AA/SL/al