LEGISLATIVE EDUCATION STUDY COMMITTEE
BILL ANALYSIS
55th Legislature, 2nd Session, 2022

Bill Number HB122/HECS **Sponsor** HEC

Tracking Number .222491.1 **Committee Referrals** HEC/HAFC

Short Title School Cybersecurity Program

Analyst García/Simon **Original Date** 2/7/2022
Last Updated

BILL SUMMARY

Synopsis of Bill

House Bill 122 (HB122/HECS) appropriates funds to the Department of Information Technology (DoIT) for the development of a cybersecurity program for all school districts, charter schools and state special schools and a statewide education technology infrastructure network by end of FY26.

FISCAL IMPACT

HB122/HECS appropriates $45 million from the general fund to DoIT for expenditure from FY23-FY26. Any unexpended or unencumbered balance remaining at the end of FY26 shall revert to the general fund. The bill outlines how the funds shall be distributed annually to implement and maintain the cybersecurity program across 87 school districts and 73 charter and 3 state special schools as follows:

- For FY23, expenditure of $8 million to set up cybersecurity program for a minimum of 35 school districts and 18 charter or state special schools;
- For FY24, expenditure of $10 million to maintain cybersecurity programs and expand to a minimum of an additional 20 school districts and 18 charter or state special schools;
- For FY25, expenditure of $12 million to maintain program extending to a minimum of an additional sixteen school districts and eighteen charter or state special schools;
- FY26, expenditure of $15 million to maintain and extend program to the remaining school districts, charter schools and state special schools that were not included in the FY23 through FY25 expenditures.

The Public Education Department (PED) notes HB122/HECS allows the department to fund 3 FTE from the annual appropriations, but the department anticipates 6 FTE will be needed. The department further states the 6 FTE should be added to PED's operating budget for FY27 and subsequent years. However, PED notes limited capacity at the department and suggests PED may not be the ideal agency to manage cybersecurity projects. With the appropriation being made to DoIT, PED will work closely with the DoIT to implement the provisions of HB122/HECS.

DoIT similarly notes, due to PED's lack of experience in developing cybersecurity systems, the department will face challenges in carrying out the provision of HB122/HECS, leading to considerable inefficiencies. Additionally, DoIT suggests a statewide initiative to address cybersecurity issues would generate efficiencies, economies of scale, and resource preservation that could be lost if the state undertakes initiatives targeted to a single department or sector.

SUBSTANTIVE ISSUES

HB122/HECS includes funding to support cybersecurity programs for school districts, charter schools and state special schools. The locally chartered charter schools are technically part of the school district authorizing the charter school and possibly are meant to be served through the school district.

Statewide Education Network. The appropriation in HB122/HECS would authorize DoIT to develop and implement a cybersecurity program for the statewide education technology network authorized under the Public School Capital Outlay Act. That law requires the Public School Capital Outlay Council (PSCOC) to develop guidelines that may be used to fund educational technology infrastructure projects. However, the current law does not require any entity to develop, maintain, or operate a statewide education technology infrastructure network. As of January, PSCOC has not yet adopted guidelines for a network, although the Public Schools Facilities Authority (PSFA) has developed draft guidelines for consideration at PSCOC's March meeting. PED notes department staff have participated in a limited capacity in planning meetings for a statewide technology infrastructure network, but the department may not be the best state agency to lead the network's cybersecurity program.

PED suggests additional clarity as to which state agency is responsible for operating the statewide education network would be beneficial. PSFA notes the recently created Office of Broadband at DoIT may be better suited to manage cybersecurity programs.

Cybersecurity Issues. Cyberattacks are a serious and consistent threat to public schools. One survey from the National School Boards Association found school officials are less prepared for cyberattacks than their peers in private sector companies. 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. 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.

Currently, cybersecurity is a local responsibility, managed by the school district or charter school. PED's current role is to support individual school districts and charter schools in implementing cybersecurity best practices. PED reports recent ransomware attacks have targeted Albuquerque, Truth or Consequences, Bernalillo, Las Cruces, and Gadsden. In FY22, PED received $1.5 million

for cybersecurity, which the department used for vulnerability scanning, in-depth training, and to respond to emergencies.

ADMINISTRATIVE IMPLICATIONS

PED suggests HB122/HECS would require a new PED division dedicated to cybersecurity. The unit would establish a security operations center to carry out the provisions of HB122/HECS and would require constant communication and collaboration with PSFA and DoIT to maintain a high level of security for the State Education Network. To align with best practice, DoIT suggests the program proposed by HB122/HECS should include specific goals, benchmarks, measures, and provisions to govern planning and oversight.

RELATED BILLS

Relates to Senate Bill 98, which would establish a cybersecurity office within DoIT and require statewide cybersecurity standards and planning, including for public schools.

SOURCES OF INFORMATION

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

JJG/ctf/mb