LFC Requester:	Hitzman

AGENCY BILL ANALYSIS
2023 REGULAR SESSION

SECTION I: GENERAL INFORMATION

Check all that apply:

Original X **Amendment** ____ **Date Prepared**: 02/16/23

Correction ___ **Substitute** ____ **Bill No:** HB388

Sponsor: Sariñana **Agency Name and Code Number**: PED - 924

Short Title: CYBERSECURITY FUND **Person Writing** Gregory Frostad

Phone: (505) 470-5752 **Email:** gregory.frostad@ped.nm.gov

SECTION II: FISCAL IMPACT

APPROPRIATION (dollars in thousands)

Appropriation		Recurring or Nonrecurring	Fund Affected
FY23	FY24		
0	$35,000.00	Non-recurring	General Fund

(Parenthesis ( ) Indicate Expenditure Decreases)

REVENUE (dollars in thousands)

Estimated Revenue			Recurring or Nonrecurring	Fund Affected
FY23	FY24	FY25		
None	None	None	N/A	NFA

(Parenthesis ( ) Indicate Expenditure Decreases)

ESTIMATED ADDITIONAL OPERATING BUDGET IMPACT (dollars in thousands)

	FY23	FY24	FY25	3 Year Total Cost	Recurring or Nonrecurring	Fund Affected
Total	None	None	None	N/A	N/A	NFA

(Parenthesis ( ) Indicate Expenditure Decreases)

Duplicates/Relates to Appropriation in the General Appropriation Act

SECTION III: NARRATIVE

BILL SUMMARY

Synopsis: House Bill 388 (HB388) would establish a Cybersecurity Fund to be used for cyber-attack response and recovery services of information technology systems or databases that are operated by any branch of state government, political subdivisions, public schools, or tribal entities.

FISCAL IMPLICATIONS

The bill would appropriate $35 million from the general fund to the Cybersecurity Fund for expenditure in FY24 and subsequent fiscal years for the purposes of the fund. Unexpended and unencumbered funds would not revert to the general fund a t the end of a fiscal year.

SIGNIFICANT ISSUES

Since 2018, New Mexico state and local government, hospitals, public school districts, and higher education institutions have been victim to at least 30 cybersecurity and ransomware attacks. The state has appropriated a total of $7 million to prevent cyber-attacks and manage the associated risks. However, most of those dollars have supported planning and pilot-type activities within DoIT, and very few widespread protections for state government agencies have been set into place. In a 2020 memo, Legislative Finance Committee (LFC) staff recommend DoIT develop a state cybersecurity plan that outlines the state's disaster management plan and cybersecurity posture.

Public School Related Cyberattacks
2018-2020

Date	School District / Agency	Cyber Issue	Cost
9/2018	Public Education Department	Phishing and spoofed email requests for payroll changes from the PED.	N/A
9/2018	Santa Fe Public Schools	NM Office of the State Auditor received reports of potential criminal violations & suspected fraud associated with phishing & spoofed email requests for payroll changes.	Unknown
9/2018	Christine Duncan Charter School (Albuquerque)	Phishing scam. Fraudulent emails appearing to come from the principal attempting to 'phish' financial account information.	N/A
1/2019	Las Cruces Public Schools	School system forced to disable network to stop spread of cyberattack. IT officials discovered infected servers & promptly removed them from network. Over 1,000 school are believed to have been attacked in total.	$300,000
7/2019	Gadsden Independent School District	Dozens of seniors did not after district officials discovered students hacked into district system and changed grades from February through April. 456 grades from various levels had been altered. Of the 55 students found responsible, 29 were seniors, and 26 were in 10th or 11th grade. Five were suspended & the others have various options to rectify their work.	Unknown
7/2019	Gadsden Independent School District	Ransomware attack prompted staff to shut down the internet and phone service. The effect of ransomware, RUYK.	$1.9 million in restoration
9/2019	Rio Rancho Public Schools	DDOS attack (denial of service). Overloading of network with large amount of data to make system crash and shut down all online sites.	Unknown
9/2019	Las Cruces Public	LCPS confirmed it accidentally sent out an	Unknown

	Schools	email containing social security numbers of vendors. Vendors advised to place fraud alert on their credit files as a precaution, and to check credit reports and financial history for signs of identity theft.	
2/2020	Taos Municipal Schools	Hackers demanded $5000 in cash ransom for return of the control to their digital services. Emails, class instruction & the district website were disabled as part of the attack. No money paid. District working with FBI to find responsible party.	Unknown
7/2020	Clovis Municipal Schools	One of several public entities in NM targeted in a payroll phishing scam, scammers did not get any money.	Unknown
7/2020	Albuquerque Public Schools	Volcano Vista High School network knocked offline by a malicious actor. School administration believed it to be a student or students.	Unknown

Source: PED Files

With seven attacks in 2018 and 15 attacks in 2019, the number of cyberattacks in New Mexico has continued to increase. However, New Mexico lacks protections deemed best practices by other states or national organizations, including processes for reporting cyber incidents, and mandatory training for employees. For example, NM does not have a uniform cybersecurity process for reporting cyber incidents, or for entities seeking assistance. In Iowa, 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 Iowa 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, and the National Conference of State Legislatures (NCSL) reports that while every state offers cybersecurity training for state employees, it is only mandatory for employees in 16 states. 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. DoIT reports that in February 2020, they notified IT leads and state agency Chief Information Officers (CIOs) of the department's cybersecurity awareness training initiatives available to state agencies beginning in March of that year. However, due to COVID-19, DoIT postponed the training.

PERFORMANCE IMPLICATIONS

None.

ADMINISTRATIVE IMPLICATIONS

None.

CONFLICT, DUPLICATION, COMPANIONSHIP, RELATIONSHIP

Relates to: SB280, Cybersecurity Act, which would create a new Cybersecurity Office.

TECHNICAL ISSUES

It is not clear how entities other than legislative state agencies, judicial state agencies, and executive state agencies would request or receive access to this funding, including local school districts.

OTHER SUBSTANTIVE ISSUES
The Department of Homeland Security (DHS) and the National Association of State Chief Information Officers (NASCIO) believe that cybersecurity should be governed as a strategic enterprise across state government and other public sectors in six areas: workforce and education, strategy and planning, budget and acquisition, risk identification and mitigation, incident response, and information sharing. An NCSL survey of top IT security officers in all 50 states identified the top three issues affecting states' cybersecurity: budget, talent, and increasing cyber threats. While any individual, government, or business is a potential victim, school systems are particularly vulnerable because they hold troves of private data, and school districts often lack the resources to fend off intruders.

ALTERNATIVES
Pursuing Cyber insurance to cover the entities stated in the bill may be an alternative or could be included as an additional use for the fund.

WHAT WILL BE THE CONSEQUENCES OF NOT ENACTING THIS BILL
None.

AMENDMENTS
None.