FISCAL IMPACT REPORT

SPONSOR HGEIC **LAST UPDATED**
ORIGINAL DATE 02/25/23
SHORT TITLE Cybersecurity Fund **BILL NUMBER** CS/House Bill 388/HGEICS
ANALYST Hitzman

ESTIMATED ADDITIONAL OPERATING BUDGET IMPACT*
(dollars in thousands)

	FY23	FY24	FY25	3 Year Total Cost	Recurring or Nonrecurring	Fund Affected
DoIT Admin & Operations	No fiscal impact	$276.0	$276.0	$552.0	Recurring	General Fund

Parentheses ( ) indicate expenditure decreases.
*Amounts reflect most recent analysis of this legislation.

Relates to Senate Bills 280 and 269
Relates to appropriation in the General Appropriation Act of 2023

Sources of Information

LFC Files

FBI – *Internet Crime Report 2021*
Pew Charitable Trusts - *States Weigh Bans on Ransomware Payoffs (2021)*
National Conference of State Legislatures – *Cybersecurity Legislation 2022*
IBM – *Cost of a Data Breach Report 2022*

Responses Received From
Department of Public Safety (DPS)
New Mexico Corrections Department (NMCD)
Regulation and Licensing Department (RLD)
Attorney General (NMAG)
State Treasurer's Office (STO)
Higher Education Department (HED)
Department of Information Technology (DoIT)

SUMMARY

Synopsis of HGEIC Substitute for House Bill 388

The House Government, Elections and Indian Affairs Committee substitute for House Bill 388 (HB388) creates the cybersecurity fund as a nonreverting fund in the state treasury to be administered by the Department of Information Technology (DoIT) for cyber-attack response

and recovery services of information technology systems or databases owned or operated by any branch of state government, political subdivisions, public schools, and tribal entities. The bill provides that, upon enactment of Senate Bill 280, the cybersecurity office shall promulgate rules to govern and administer the cybersecurity fund. The rules shall specify the application process, criteria, review process, and requirements for reversions.

This bill does not contain an effective date and, as a result, would go into effect June 16, 2023, (90 days after the Legislature adjourns) if signed into law.

FISCAL IMPLICATIONS

Although the bill does not provide an appropriation, the bill creates a new fund and provides for continuing appropriations. LFC has concerns with including continuing appropriation language in the statutory provisions for newly created funds because earmarking reduces the ability of the Legislature to establish spending priorities.

It is unknown how much funding would be needed to support the intended functions for all eligible entities. The Regulation and Licensing Department (RLD), for example, experienced a cyberattack in late 2022 and estimated the cost of recovery to total around $3.5 million. Because it is unknown the extent to which the fund would be utilized each year, ongoing expenditures from the fund are nearly impossible to determine at this time.

It is also unknown if DoIT or the cybersecurity office would have the administrative capacity to administer and oversee funds to other entities. However, DoIT estimates, "The office will need to hire 2 additional FTE to manage and administer the program. DoIT's FY23 operating budget has 5 FTE related to cybersecurity and LFC reported the average FTE cost is $138 thousand per FTE. Therefore, the cost for 2 FTE such as an IT business analyst and financial coordinator would be $276 thousand per year." This cost is scored as a recurring cost to the general fund.

The State Treasurer's Office (STO) notes "creating a new fund in the state treasury is inconsequential and does not have a fiscal impact on STO. Timing, collaboration, and communication between agencies and STO is critical when transferring/wiring funds."

SIGNIFICANT ISSUES

According to the Federal Bureau of Investigation's (FBI) annual Internet Crime Report, over the past decade New Mexico has seen an increase in losses related to cybersecurity incidents of $10.1 million, or 20 percent. For example, New Mexico saw a total of 3,427 reported cybersecurity victims in 2020 for losses of $23.9 million and 2,644 victims in 2021 for losses of $12.7 million. Comparatively, in 2011, the FBI estimated New Mexico's complainant losses to total only $2.6 million.

A "cyberattack" can include instances in which a malicious actor can gain access to emails, user files, contacts, and personal information, can add or delete files from someone's computer, can download or inject additional malicious software without the user's knowledge, and can deplete system resources—like power or bandwidth—by overloading a system network with traffic. The victims may not be able to trace the source of the malicious code or application and may not be able to navigate their network if the malicious actor has modified security codes or passwords.

Hackers who use ransomware, for example, use this tactic to take control of system networks or data and require a ransom sum of money be paid to retrieve the data or release the system from the hacker's control. Ransomware is increasing in prevalence over time, having only first been reported on in 2012 for losses of $134 thousand, whereas in 2021 those losses have increased over 360 percent to total $49.2 million.

Further, DoIT notes the following:

> HB388 provides support for cyber-attack response and recovery. The cost of cyber-attacks can vary from $3.8 million to $4.8 million and more depending on the complexity of the attack and what type of data was at risk. The estimated cost to recover from a recent cyber-attack is over $3.6 million. Based on the IBM 2022 Cost of a Data Breach report, a cyber breach in healthcare can cost over $10 million.

The bill allows the money within the cybersecurity fund to be used for "cyber attack response and recovery services," but does not define what constitutes those specific services. The bill does not specify any particular types of attacks that would be eligible for recovery and response services nor does it clarify what level of severity an attack must meet in order for funds to be used. Further, as written, the bill also does not provide details regarding what can and cannot be funded, such as ransom payments. The PEW Charitable Trusts notes, as of 2021, three states were considering legislation that would ban state and local government agencies from paying ransom if attacked by cyber criminals. Senators from Pennsylvania, for example, noted banning ransom payments would make the state less attractive for cyber criminals if they know they will not get paid.

Other states have proposed dedicated funds to address cybersecurity issues. For instance, Maryland passed legislation to establish the local cybersecurity support fund as a special, non-reverting fund. However, the fund was more broadly proposed to help provide financial assistance to local governments to improve cybersecurity preparedness, rather than being explicitly for response and recovery actions as proposed in SB452. A fund proposed in New York—the cyber security enhancement fund—would be used to upgrade cybersecurity in local governments and restricts the use of taxpayer moneys in paying ransoms in response to ransomware attacks. That legislation is pending.

The Department of Public Safety (DPS) notes "criteria utilized by the DoIT Cabinet Secretary or State [Chief Information Security Officer] CISO to authorize the use of the funds are not addressed in the bill. HB388 does not address how agencies would request fund expenditures."

The Higher Education Department (HED) notes:

> A statewide Cybersecurity Office would have benefits for New Mexico's Public Higher Education Institutions (HEIs). All HEIs collect and manage sensitive information about students, staff, faculty, and research. This includes personal information, financial information, academic information, and health-related information. A statewide Cybersecurity Office could set and monitor cybersecurity requirements and standards to protect this information and data as well as help mitigate ransomware and other disruptive and destructive cybersecurity breaches at HEIs.
>
> Cybersecurity has been a challenge for all NM HEIs, many of which experienced serious breaches as a result of cyber attacks in the last three years. These breaches resulted in disruption of student services and loss of data. NMHED sponsors and assists in securing

> State and Federal funding for HEI cybersecurity. NMHED provides no cybersecurity technical assistance to New Mexico HEIs. HEIs are responsible for their own cybersecurity. Many of the smaller New Mexico colleges do not have the resources or expertise to fully manage their cybersecurity needs, and often rely on outside help to ensure their networks and systems are secure. By providing centralized optional cybersecurity services and resources, SB280 could help reduce and in some cases prevent disruption and loss in higher education caused by cyber attacks.

Similarly, HB388 could help reduce the burden on education entities for pursuing cyber response and recovery services and could assist in covering losses. DoIT notes, "Cyber-breach insurance that is available in the private sector to cover the costs and losses associated with cybersecurity events is unavailable to New Mexico governmental bodies. Self-insuring, or funding, such as what is proposed by HB 388, is the only option for public sector cyber incident response costs."

However, the bill creates a new fund but does not provide an appropriation for the fund, so it is unclear when the funding awards would be initially administered. It will likely take time for the office to create rules governing the uses of the fund, so the office may not be ready to administer the funds until the next fiscal year, at which point the fund could receive additional appropriations to support grant awards if not elsewhere funded during the 2023 legislative session.

IBM produces reports on the cost of a data breach, and in 2022 IBM noted the costs for addressing cyberattacks were significantly reduced if the entity used an incident response plan and testing, by around 58 percent. The bill does not provide for the department to implement or develop an incident response plan to address cyberattacks in conjunction with the usage of the fund. However, other proposed legislation amending the Department of Information Technology Act will allow DoIT broader authority over implementing cybersecurity services if passed, which could include incident response as an additional duty of the department. However, HB388 notes the fund would be administered by the cybersecurity office once created, rather than DoIT, so it is unclear whether those changes to the DoIT Act to broaden its authorities would continue to apply (if passed) or if those authorities would still be necessary if the office is created.

ADMINISTRATIVE IMPLICATIONS

The bill provides that the cybersecurity office will develop rules to determine how agencies or other entities are to access funds, likely through some grant process. DoIT and the office will need to "go through a rule making process to further define what cost would be covered and what would be the process to track and report on the expenditure."

CONFLICT, DUPLICATION, COMPANIONSHIP, RELATIONSHIP

The bill relates to SB280, which would create the cybersecurity office within DoIT. HB388 is a companion, so DoIT notes SB280 must be enacted in order for HB388 to take effect. The bill also relates to SB269, which expands departmental authorities regarding cybersecurity services.

The bill also relates to an appropriation in the General Appropriation Act of 2023, which appropriates $10 million to DoIT for cybersecurity services, including up to $3 million to be used for incident response at RLD, as well as $3 million to DoIT for cybersecurity services at

higher education and $2.5 million at public education institutions.

ALTERNATIVES

Appropriations could be made in the General Appropriation Act of 2023 to address cybersecurity response and recovery, either at particular agencies or within DoIT, without creating a new fund.

DoIT notes the following:

> Instead of general fund, there could be potential use of revenue from the cannabis fund to support cybersecurity incident response and recovery. In the future, this fund could be used to support other and future federal cyber grants as state's share of the grant match, if designated by the Legislature.

WHAT WILL BE THE CONSEQUENCES OF NOT ENACTING THIS BILL

RLD notes "in the event a New Mexico governmental entity, such as a state agency or department, experiences a cyber attack, the governmental entity will continue to be required to attempt to cover the costs of responding and recovering from that cyber attack from the governmental entity's own budget, and then seek emergency funding from the Legislature to address any budget shortfalls."

JH/mg/hg/mg