FISCAL IMPACT REPORT

SPONSOR Sariñana **LAST UPDATED** **ORIGINAL DATE** 1/22/24

SHORT TITLE Create Cybersecurity Fund **BILL NUMBER** House Bill 72

ANALYST Hilla

APPROPRIATION*
(dollars in thousands)

FY24	FY25	Recurring or Nonrecurring	Fund Affected
	$35,000.0	Recurring	General Fund

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

ESTIMATED ADDITIONAL OPERATING BUDGET IMPACT*
(dollars in thousands)

Agency/Program	FY24	FY25	FY26	2 Year Total Cost	Recurring or Nonrecurring	Fund Affected
DoIT		$300-$400	$300-$400	$600-$800	Recurring	General Fund

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

Sources of Information

LFC Files

Agency Analysis Received From
Department of Information Technology (DoIT)
State Treasurer (STO)

SUMMARY

Synopsis of House Bill 72

House Bill 72 (HB72) appropriates $35 million from the general fund to the cybersecurity fund for expenditure in FY25 and subsequent years for cyber-attack response and recovery of information technology systems owned or operated by an agency of the executive, legislative, or judicial branch of state government, a political subdivision of the state, or a tribal entity. Any unexpended balances shall not revert to the general fund.

This bill does not contain an effective date and, as a result, would go into effect 90 days after the Legislature adjourns, or May 15, 2024, if enacted.

FISCAL IMPLICATIONS

This 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.

The Department of Information Technology (DoIT) notes that the Office of Cybersecurity projects the need of 2 to 3 FTE to manage and administer the program at approximately $125-150 thousand per individual per year for a total of $300-$400 thousand in each FY25 and FY26. DoIT also notes that since the appropriation is nonrecurring, the bill is unclear how cybersecurity efforts will continue if the fund is depleted.

The State Treasurer indicates this fund has no direct fiscal impact on the agency, but it does increase the workload of their staff and that timing, collaboration, and communication between agencies are fundamental when transferring money.

SIGNIFICANT ISSUES

DoIT notes the cost of cyber-attacks varies, but typically are several millions of dollars depending on the complexity and type of attack. The estimated cost to recover from a recent cyber-attack of a New Mexico state agency was over $3.6 million, and the IBM 2022 Cost of a data Breach report found that a cyber breach in healthcare can cost more than $10 million. State agencies themselves do not have funds in their budgets for cyber-attacks, but DoIT states many local governments and educational entities have self-insurance funds to pay for cyber-security attacks that typically cover the first million dollars or more.

LFC's 2023 analysis regarding similar proposed cybersecurity fund (House Bill 388), found similar issues regarding the significant issues of HB72 which are: HB72 does not define what constitutes "cyber-attack response and recovery services." HB72 does not specify any types of attacks that would be eligible for recovery nor what level of attack is needed for funds to be dispersed, but rather leaves the promulgation of rules to the office of cybersecurity.

Additionally, provisions of the bill are reactive, not preventative for cyber-attacks. It takes a top-down approach to cybersecurity and seeks to cure attacks rather than cure *and* prevent them. Outlining preventative measures for cybersecurity under the office of cybersecurity should be included in the bill to further mitigate the need for cyber response and recovery.

ADMINISTRATIVE IMPLICATIONS

DoIT states that the office of cybersecurity will need to create memorandums of understanding to work with various political subdivisions.

OTHER SUBSTANTIVE ISSUES

DoIT says cyber-breach insurance that is available in the private sector to cover the costs and losses with cybersecurity breaches/attacks are unavailable to New Mexico state agencies but notes the increases of cyber insurance and deductibles make self-insuring/funding a good cost-effective option for the public sector to manage cyber incidents.

WHAT WILL BE THE CONSEQUENCES OF NOT ENACTING THIS BILL

DoIT mentions that if HB72 is not enacted, tribal entities, political subdivisions, and state agencies may independently seek recovery funding from the Legislature, but it could lack adequate and effective oversight and may not result in the best practices of cybersecurity implementation.

EH/al/ne/ss