LFC Requester:	Hilla

AGENCY BILL ANALYSIS
2024 REGULAR SESSION

WITHIN 24 HOURS OF BILL POSTING, UPLOAD ANALYSIS TO:

Analysis.nmlegis.gov

{Analysis must be uploaded as a PDF}

SECTION I: GENERAL INFORMATION
{Indicate if analysis is on an original bill, amendment, substitute or a correction of a previous bill}

Check all that apply:
Original X **Amendment** ____
Correction ___ **Substitute** ____

Date 1/17/2024
Bill No: HB 72

Sponsor: Debra M. Sarinana
Short Title: Cybersecurity Fund

Agency Name and Code Number: Dept. of Information Technology - 36100
Person Writing Raja Sambandam
Phone: 505-660-3280 **Email** Raja.sambandam@doit.nm.gov

SECTION II: FISCAL IMPACT

APPROPRIATION (dollars in thousands)

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

(Parenthesis ( ) Indicate Expenditure Decreases)

ESTIMATED ADDITIONAL OPERATING BUDGET IMPACT (dollars in thousands)

	FY24	FY25	FY26	2 Year Total Cost	Recurring or Nonrecurring	Fund Affected
Total		$300-450	$300-450	$600-900	Recurring	General Fund

(Parenthesis ( ) Indicate Expenditure Decreases)

Duplicates/Conflicts with/Companion to/Relates to:
Duplicates/Relates to Appropriation in the General Appropriation Act

SECTION III: NARRATIVE

BILL SUMMARY

Synopsis:

House Bill (HB) 72 creates the Cybersecurity Fund from the general fund as a non-reverting fund in the State Treasury to be administered by the Office of Cybersecurity ("OCS") for the purposes stated in Subsection B of the bill.

Subsection B states: Money in the cybersecurity fund shall be used for cyber-attack response and recovery services of information technology systems or databases operated or owned by an agency of the executive, legislative or judicial branch of state government, a political subdivision of the state or a tribal entity. The OCS shall promulgate rules to govern administration of the cybersecurity fund.

The fund is for expenditure in FY 2025 and subsequent fiscal years for the purposes of the fund. Any unexpended or unencumbered balance remaining at the end of a fiscal year shall not revert to the general fund.

FISCAL IMPLICATIONS

The OCS projects a need to hire 2-3 FTE to manage and administer the program at an approximate cost of $125-150 thousand per year, per individual.

HB 72 provides that the fund consists of appropriations, bequests, distributions, donations, gifts, grants or money that otherwise accrues to the fund. However, the appropriation is nonrecurring, and the bill is unclear about how to continue the cybersecurity efforts prescribed by the bill if the fund is depleted.

SIGNIFICANT ISSUES

HB 72 provides support for cyber-attack response and recovery. The costs of cyber-attacks can vary, but they are typically in the several millions of dollars, 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 of a New Mexico state agency was 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.

While state agencies do not have funds in their budget to cover the costs related to a cyber-attack, many of the local governments and educational entities have self-insurance funds to pay for cyber-attacks that typically covers the first million dollars or more.

PERFORMANCE IMPLICATIONS

ADMINISTRATIVE IMPLICATIONS

The OCS will likely need to develop an appropriate memorandum of understanding to work with various political subdivisions.

CONFLICT, DUPLICATION, COMPANIONSHIP, RELATIONSHIP

TECHNICAL ISSUES

OTHER SUBSTANTIVE ISSUES –
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 state agencies.

However, the rising cost of cyber insurance and increasing deductibles make self-insuring, or funding, the cost-effective option for the public sector to manage cyber incident response costs.

ALTERNATIVES

WHAT WILL BE THE CONSEQUENCES OF NOT ENACTING THIS BILL

If this bill is not enacted, state agencies, political subdivisions, and tribal entities may independently seek incident response and recovery funding from the Legislature. Such an approach may lack adequate and effective oversight and may not result in the implementation of cybersecurity best practices or the attainment of necessary economies of scale.

AMENDMENTS

HB 72 as currently drafted provides funding only for *reactive* response to and recovery from a cyber-attack. HB 72 should be amended to also provide for proactive protection of state agencies, political subdivisions and tribal entities by including the following underlined language:

Section 1. B. Money in the cybersecurity fund shall be used <u>to identify and manage cybersecurity risk, protect critical infrastructure, and detect suspicious or malicious activity, and</u> for cyber-attack response and recovery services of information technology systems or databases operated or owned by an agency of the executive, legislative or judicial branch of state government, a political subdivision of the state or a tribal entity.