

Fiscal Note

BILL # HB 2690

TITLE: cybersecurity risk; insurance

SPONSOR: Weninger

STATUS: House Engrossed

PREPARED BY: Rebecca Perrera

Description

The bill establishes the Cyber Risk Insurance Fund administered by the Arizona Department of Administration (ADOA) and requires ADOA to obtain insurance for actual or suspected data breaches or cyber incidents. In addition, the bill allows ADOA to impose premiums and deductibles on state agencies and requires the department to include the actuarial needs for replenishment of the fund in the agency's annual budget request.

Estimated Impact

We estimate that ADOA's annual cost of administering a Cyber Risk Insurance Program would be \$3.0 million. This amount includes the annual premium and administration. In addition, we estimate that the bill would require ADOA to establish reserves to pay any deductibles associated with the bill. That projected cost is \$20 million. Both the annual operating cost and the deductible reserve estimate are consistent with the Executive's FY 2023 budget request. The Executive would fund these costs with a transfer from the Risk Management Revolving Fund.

While the Risk Management Fund has sufficient reserves to pay the initial costs, state agencies are expected to be billed annually to finance the ongoing operations of the Cyber Risk program. We anticipate that the General Fund share of this cost would be about 50% of the annual cost, or \$1.5 million starting in FY 2025.

If the state has to pay out the deductible, the reserve would need to be replenished. The General Fund could be expected to pay 50% of that cost as well.

Analysis

A.R.S § 18-552 currently requires ADOA to investigate any instance of a state agency "cyber incident," which is broadly defined as an event that creates reasonable suspicion that an Information Technology (IT) system may have been compromised or cybersecurity controls may have failed. If investigation of the incident confirms unauthorized access that materially compromised the security or confidentiality of data in an IT system, the incident becomes a "cyber breach," which triggers certain actions the state is required to take such as investigating and notifying individuals affected. A cybersecurity insurance program as established by the bill would pay for the state response in the event of an incident or breach.

The \$3.0 million of annual operating costs include \$137,400 for 1 FTE Position and \$2.9 million for third-party excess insurance. ADOA intends to procure private cyber insurance to cover excess losses not covered by the Cyber Risk Insurance Fund.

We assume that ADOA would then start charging agencies in FY 2025. Allocations could be based on risk factors including number of records, IT applications, and FTE Positions. We anticipate that the General Fund share of this cost could be 50% of the annual cost, or \$1.5 million.

(Continued)



Currently, state agencies, including the universities, pay independently for cyber insurance. Total agency premiums are \$1.3 million annually. As a result, there could be some small offsetting savings from eliminating these premiums, but the cost savings depends on which agencies participate in the new program and ADOA's methodology to allocate premiums.

Local Government Impact

None

3/10/22