BILL ANALYSIS

H.B. 4996
By: Bell, Cecil
State Affairs
Committee Report (Unamended)

BACKGROUND AND PURPOSE

Cybersecurity threats have, regrettably, become the new normal and the risks can be daunting even for the most sophisticated prevention software available. When a breach compromises critical data, and sensitive and personal information, the mitigation that follows becomes paramount. Moreover, limiting financial exposure is a must.

When the Department of Information Resources (DIR) collects cyber data, it does so for state leaders to determine how best to use that information to prevent and mitigate threats to the state. But an important next step is to instruct DIR and the State Office of Risk Management to test the insurance market to determine the viability of placing cybersecurity insurance for the state. Cybersecurity insurance is an essential tool utilized by thousands of private businesses and governmental entities to minimize the enormous potential financial hit to any organization, including disparate state agencies.

H.B. 4996 seeks to allow DIR to gather data via assessments of every state agency and then take that information to the market to determine the cost/benefit of utilizing cyber insurance as a tool of risk management for the state.

CRIMINAL JUSTICE IMPACT

It is the committee's opinion that this bill does not expressly create a criminal offense, increase the punishment for an existing criminal offense or category of offenses, or change the eligibility of a person for community supervision, parole, or mandatory supervision.

RULEMAKING AUTHORITY

It is the committee's opinion that this bill does not expressly grant any additional rulemaking authority to a state officer, department, agency, or institution.

ANALYSIS

H.B. 4996 requires the Department of Information Resources (DIR), not later than October 1, 2023, to contract with a cyber risk model vendor to conduct a study on the development of a statewide risk framework in order to determine the need for and feasibility of implementing a statewide cyber insurance program. The bill requires DIR to enter into a memorandum of understanding with the State Office of Risk Management (SORM) to support this assessment and authorizes SORM, based on the results of the study, to develop and maintain a statewide cyber insurance program meeting the specifications identified in the study.

H.B. 4996 requires DIR, not later than April 1, 2024, and in conjunction with SORM, to prepare and submit to the governor and the legislature a report containing the results of the study and any recommendations for legislative or other action to address the need for and feasibility of requiring cyber insurance.

H.B. 4996 defines "risk framework" as key security domains identified by cyber insurance underwriters based on current security controls and specifies that "security controls" include use of multiple security levels, managing user access, user authentication, network and server vulnerability, malware defense, operational technology, remote work, third-party vendor management, email filtering, response planning, data encryption and backup, use of wireless devices and connections, monitoring users or devices, continuity of service, incident response, appropriate insurance coverage, and governance. The bill's provisions expire September 1, 2025.

EFFECTIVE DATE

On passage, or, if the bill does not receive the necessary vote, September 1, 2023.