Department of Legislative Services

Maryland General Assembly
2025 Session

FISCAL AND POLICY NOTE
First Reader

House Bill 235 (Chair, Health and Government Operations Committee)(By Request - Departmental - Information Technology)

Health and Government Operations

State Government - Information Technology - Cybersecurity Revisions

This departmental bill makes various clarifying and administrative changes to the State's regulatory framework governing State and local cybersecurity, generally clarifying and distinguishing the responsibilities between the Department of Information Technology (DoIT) and Maryland Department of Emergency Management (MDEM).

Fiscal Summary

State Effect: The bill's requirements can be handled using existing budgeted resources. Revenues are not affected.

Local Effect: The bill does not materially affect local government operations or finances.

Small Business Effect: DoIT has determined that this bill has minimal or no impact on small business (attached). The Department of Legislative Services concurs with this assessment.

Analysis

Bill Summary/Current Law: Chapters 241, 242, and 243 of 2022 expanded and enhanced the State's regulatory framework for State and local government cybersecurity. Among other things, the Acts required additional funding for cybersecurity, established leadership positions in State government for cybersecurity, codified existing cybersecurity

requirements from a previous executive order, and requiring State and local governments to perform cybersecurity preparedness assessments. Directly relevant to the bill, the Acts:

- established the Cyber Preparedness Unit (CPU) within MDEM and require the unit to, among other duties, support local governments in developing a vulnerability assessment and cyber assessment and develop and regularly update an online database of cybersecurity training resources, including specified resources;
- codified and expanded the duties of the Office of Security Management (OSM) within DoIT;
- required OSM to provide an annual report with specified information about the office's cybersecurity activities to specified committees of the General Assembly; and
- specified the duties of the Secretary of Information Technology as they related to cybersecurity.

The bill modifies the State's regulatory cybersecurity framework by:

- transferring the responsibility for supporting local governments in developing vulnerability assessments and cyber assessments from CPU to OSM;
- repealing the requirement that CPU develop and regularly update training resources for local governments related to malware and ransomware detection;
- clarifying that OSM may take or direct actions required to a mitigate a threat affecting or potentially affecting an entity connected to the State-owned Internet network when a connection *may* introduce a serious risk to other entities connected to the network;
- clarifying that OSM is not responsible assisting specified local government entities in the development of cybersecurity preparedness and response plans;
- repealing the requirement that OSM's annual report include (1) an analysis of the State's expenditures on cybersecurity relative to overall information technology spending for the prior three years and (2) recommendations for changes to the budget, including amount, purpose, and timing to improve State and local cybersecurity preparedness; and
- clarifying that the Secretary of Information is responsible for implementing information technology policies, procedures, and standards and a statewide cybersecurity strategy in addition to developing, maintaining, revising, and enforcing the policies, procedures, and standards, and developing and maintaining the strategy.

Background: DoIT advises that the bill is necessary to clarify the roles and responsibilities of DoIT and MDEM with respect to the cybersecurity services and supports established by the Chapters 241, 242, and 243 of 2022.

DoIT advises that the bill's changes reflect the areas of expertise of each agency, ensuring that DoIT is responsible for the highly technical cybersecurity work and MDEM is responsible for assisting local governments with planning and exercising activities. MDEM advises that the bill's changes reflect the current practices and activities of CPU.

Additional Information

Recent Prior Introductions: Similar legislation has not been introduced within the last three years.

Designated Cross File: SB 244 (Chair, Education, Energy, and the Environment Committee)(By Request - Departmental - Information Technology) - Education, Energy, and the Environment.

Information Source(s): Department of Information Technology; Maryland Department of Emergency Management; Baltimore, Carroll, and St. Mary's counties; Montgomery County Public Schools; Department of Legislative Services

Fiscal Note History: First Reader - January 13, 2025
js/mcr

Analysis by: Richard L. Duncan

Direct Inquiries to:
(410) 946-5510
(301) 970-5510

ANALYSIS OF ECONOMIC IMPACT ON SMALL BUSINESSES

TITLE OF BILL: State Government - Information Technology - Cybersecurity Revisions

BILL NUMBER: HB 235

PREPARED BY: Sara Elalamy - Legislative Director

PART A. ECONOMIC IMPACT RATING

This agency estimates that the proposed bill:

_X_ WILL HAVE MINIMAL OR NO ECONOMIC IMPACT ON MARYLAND SMALL BUSINESS

OR

WILL HAVE MEANINGFUL ECONOMIC IMPACT ON MARYLAND SMALL BUSINESSES

PART B. ECONOMIC IMPACT ANALYSIS

N/A