HOUSE BILL 235

S2 5lr0198
(PRE–FILED) CF SB 244

By: **Chair, Health and Government Operations Committee (By Request – Departmental – Information Technology)**
Requested: September 19, 2024
Introduced and read first time: January 8, 2025
Assigned to: Health and Government Operations

A BILL ENTITLED

AN ACT concerning

State Government – Information Technology – Cybersecurity Revisions

FOR the purpose of altering the duties of the Cyber Preparedness Unit in the Maryland Department of Emergency Management; altering the duties of the Office of Security Management in the Department of Information Technology; altering the content of a certain report on the activities of the Office and the state of cybersecurity preparedness in the State; altering the responsibilities of the Secretary of Information Technology with regard to information technology policies and a statewide cybersecurity strategy; and generally relating to State cybersecurity.

BY repealing and reenacting, without amendments,
Article – Public Safety
Section 14–104.1(a)
Annotated Code of Maryland
(2022 Replacement Volume and 2024 Supplement)

BY repealing and reenacting, with amendments,
Article – Public Safety
Section 14–104.1(b)
Annotated Code of Maryland
(2022 Replacement Volume and 2024 Supplement)

BY repealing and reenacting, with amendments,
Article – State Finance and Procurement
Section 3.5–2A–04 and 3.5–303(a)(1) and (5)
Annotated Code of Maryland
(2021 Replacement Volume and 2024 Supplement)

EXPLANATION: **CAPITALS INDICATE MATTER ADDED TO EXISTING LAW.**
[Brackets**]** indicate matter deleted from existing law.

SECTION 1. BE IT ENACTED BY THE GENERAL ASSEMBLY OF MARYLAND, That the Laws of Maryland read as follows:

Article – Public Safety

14–104.1.

(a) (1) In this section the following words have the meanings indicated.

(2) "Local government" includes local school systems, local school boards, and local health departments.

(3) "Unit" means the Cyber Preparedness Unit.

(b) (1) There is a Cyber Preparedness Unit in the Department.

(2) In coordination with the State Chief Information Security Officer, the Unit shall:

(i) **[**support local governments in developing a vulnerability assessment and cyber assessment, including providing local governments with the resources and information on best practices to complete the assessments;

(ii)**]** develop and regularly update an online database of cybersecurity training resources for local government personnel, including technical training resources, cybersecurity continuity of operations templates, **AND** consequence management plans**[**, and trainings on malware and ransomware detection**]**;

[(iii)**] (II)** assist local governments in:

1. the development of cybersecurity preparedness and response plans;

2. implementing best practices and guidance developed by the State Chief Information Security Officer; and

3. identifying and acquiring resources to complete appropriate cybersecurity vulnerability assessments;

[(iv)**] (III)** connect local governments to appropriate resources for any other purpose related to cybersecurity preparedness and response;

[(v)**] (IV)** as necessary and in coordination with the National Guard, local emergency managers, and other State and local entities, conduct regional cybersecurity preparedness exercises; and

[(vi)**]** **(V)** establish regional assistance groups to deliver and coordinate support services to local governments, agencies, or regions.

(3) The Unit shall support the Office of Security Management in the Department of Information Technology during emergency response efforts.

Article – State Finance and Procurement

3.5–2A–04.

(a) (1) The Office is responsible for:

(i) the direction, coordination, and implementation of the overall cybersecurity strategy and policy for units of State government; and

(ii) supporting and coordinating with the Maryland Department of Emergency Management Cyber Preparedness Unit during emergency response efforts.

(2) The Office is not responsible for the information technology installation and maintenance operations normally conducted by a unit of State government, a unit of local government, a local school board, a local school system, or a local health department.

(b) The Office shall:

(1) establish standards to categorize all information collected or maintained by or on behalf of each unit of State government;

(2) establish standards to categorize all information systems maintained by or on behalf of each unit of State government;

(3) develop guidelines governing the types of information and information systems to be included in each category;

(4) establish security requirements for information and information systems in each category;

(5) assess the categorization of information and information systems and the associated implementation of the security requirements established under item (4) of this subsection;

(6) if the State Chief Information Security Officer determines that there are security vulnerabilities or deficiencies in any information systems, determine and direct or take actions necessary to correct or remediate the vulnerabilities or deficiencies, which may include requiring the information system to be disconnected;

(7) if the State Chief Information Security Officer determines that there is a cybersecurity threat caused by**, AFFECTING, OR POTENTIALLY AFFECTING** an entity

connected to the network established under § 3.5–404 of this title that introduces **OR MAY INTRODUCE** a serious risk to entities connected to the network or to the State, take or direct actions required to mitigate the threat;

(8) manage security awareness training for all appropriate employees of units of State government;

(9) assist in the development of data management, data governance, and data specification standards to promote standardization and reduce risk;

(10) assist in the development of a digital identity standard and specification applicable to all parties communicating, interacting, or conducting business with or on behalf of a unit of State government;

(11) develop and maintain information technology security policy, standards, and guidance documents, consistent with best practices developed by the National Institute of Standards and Technology;

(12) to the extent practicable, seek, identify, and inform relevant stakeholders of any available financial assistance provided by the federal government or non–State entities to support the work of the Office;

(13) provide technical assistance to localities in mitigating and recovering from cybersecurity incidents; **[**and**]**

(14) provide technical services, advice, and guidance to units of local government to improve cybersecurity preparedness, prevention, response, and recovery practices**; AND**

(15) SUPPORT LOCAL GOVERNMENTS IN DEVELOPING A VULNERABILITY ASSESSMENT AND CYBER ASSESSMENT, INCLUDING PROVIDING LOCAL GOVERNMENTS WITH THE RESOURCES AND INFORMATION ON BEST PRACTICES TO COMPLETE THE ASSESSMENTS.

(c) The Office, in coordination with the Maryland Department of Emergency Management, shall:

(1) assist local political subdivisions, including counties, school systems, school boards, and local health departments, in**[**:

(i) the development of cybersecurity preparedness and response plans; and

(ii)**]** implementing best practices and guidance developed by the Department; and

(2) connect local entities to appropriate resources for any other purpose related to cybersecurity preparedness and response.

(d) The Office, in coordination with the Maryland Department of Emergency Management, may:

(1) conduct regional exercises, as necessary, in coordination with the National Guard, local emergency managers, and other State and local entities; and

(2) establish regional assistance groups to deliver or coordinate support services to local political subdivisions, agencies, or regions.

(e) (1) On or before December 31 each year, the Office shall report to the Governor and, in accordance with § 2–1257 of the State Government Article, the Senate Budget and Taxation Committee, the Senate **[**Education, Health, and Environmental Affairs**]** Committee **ON EDUCATION, ENERGY, AND THE ENVIRONMENT**, the House Appropriations Committee, the House Health and Government Operations Committee, and the Joint Committee on Cybersecurity, Information Technology, and Biotechnology on the activities of the Office and the state of cybersecurity preparedness in Maryland, including:

(i) the activities and accomplishments of the Office during the previous 12 months at the State and local levels; and

(ii) a compilation and analysis of the data from the information contained in the reports received by the Office under § 3.5–405 of this title, including:

1. a summary of the issues identified by the cybersecurity preparedness assessments conducted that year;

2. the status of vulnerability assessments of all units of State government and a timeline for completion and cost to remediate any vulnerabilities exposed;

3. recent audit findings of all units of State government and options to improve findings in future audits, including recommendations for staff, budget, and timing;

4. **[**analysis of the State's expenditure on cybersecurity relative to overall information technology spending for the prior 3 years and recommendations for changes to the budget, including amount, purpose, and timing to improve State and local cybersecurity preparedness;

5.**]** efforts to secure financial support for cyber risk mitigation from federal or other non–State resources;

[6.**]** **5.** key performance indicators on the cybersecurity strategies in the Department's information technology master plan, including time, budget, and staff required for implementation; and

[7.**]** **6.** any additional recommendations for improving State and local cybersecurity preparedness.

(2) A report submitted under this subsection may not contain information that reveals cybersecurity vulnerabilities and risks in the State.

3.5–303.

(a) The Secretary is responsible for carrying out the following duties:

(1) developing, **IMPLEMENTING,** maintaining, revising, and enforcing information technology policies, procedures, and standards;

(5) developing**, IMPLEMENTING,** and maintaining a statewide cybersecurity strategy that will:

(i) centralize the management and direction of cybersecurity strategy within the Executive Branch of State government under the control of the Department; and

(ii) serve as the basis for budget allocations for cybersecurity preparedness for the Executive Branch of State government;

SECTION 2. AND BE IT FURTHER ENACTED, That this Act shall take effect October 1, 2025.