

SENATE BILL 244

S2

(PRE-FILED)

5lr0197
CF HB 235

By: **Chair, Education, Energy, and the Environment Committee (By Request –
Departmental – Information Technology)**

Requested: September 19, 2024

Introduced and read first time: January 8, 2025

Assigned to: Education, Energy, and the Environment

A BILL ENTITLED

1 AN ACT concerning

2 **State Government – Information Technology – Cybersecurity Revisions**

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

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

15 BY repealing and reenacting, with amendments,
16 Article – Public Safety
17 Section 14–104.1(b)
18 Annotated Code of Maryland
19 (2022 Replacement Volume and 2024 Supplement)

20 BY repealing and reenacting, with amendments,
21 Article – State Finance and Procurement
22 Section 3.5–2A–04 and 3.5–303(a)(1) and (5)
23 Annotated Code of Maryland
24 (2021 Replacement Volume and 2024 Supplement)

EXPLANATION: CAPITALS INDICATE MATTER ADDED TO EXISTING LAW.

[Brackets] indicate matter deleted from existing law.



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

3 **Article – Public Safety**

4 14–104.1.

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

6 (2) “Local government” includes local school systems, local school boards,
7 and local health departments.

8 (3) “Unit” means the Cyber Preparedness Unit.

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

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

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

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

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

20 1. the development of cybersecurity preparedness and
21 response plans;

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

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

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

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

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

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

5 **Article – State Finance and Procurement**

6 3.5–2A–04.

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

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

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

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

15 (b) The Office shall:

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

1 [6.] 5. key performance indicators on the cybersecurity strategies
2 in the Department's information technology master plan, including time, budget, and staff
3 required for implementation; and

4 [7.] 6. any additional recommendations for improving State and
5 local cybersecurity preparedness.

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

8 3.5–303.

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

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

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

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

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

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