SENATE BILL 981

F1, S2, B1 4lr2477

By: **Senator Hester**
Introduced and read first time: February 2, 2024
Assigned to: Education, Energy, and the Environment and Budget and Taxation

A BILL ENTITLED

AN ACT concerning

Local Cybersecurity Preparedness and Local Cybersecurity Support Fund – Alterations

FOR the purpose of authorizing the Governor to include in the annual budget bill a certain appropriation for certain fiscal years for the Local Cybersecurity Support Fund; requiring the Department of Information Technology to provide a certain number of regional information security officers to assist the Director of Local Cybersecurity; requiring, by a certain date, a local school system to implement certain practices regarding the network of the local school system; authorizing funds to be transferred by budget amendment from the Dedicated Purpose Account in certain fiscal years to implement this Act; and generally relating to local cybersecurity.

BY repealing and reenacting, with amendments,
Article – Public Safety
Section 14–104.2
Annotated Code of Maryland
(2022 Replacement Volume and 2023 Supplement)

BY repealing and reenacting, without amendments,
Article – State Finance and Procurement
Section 3.5–101(c), 3.5–2A–02, 3.5–301(a) and (b), and 3.5–407
Annotated Code of Maryland
(2021 Replacement Volume and 2023 Supplement)

BY repealing and reenacting, with amendments,
Article – State Finance and Procurement
Section 3.5–2A–03(e) and 3.5–405
Annotated Code of Maryland
(2021 Replacement Volume and 2023 Supplement)

SECTION 1. BE IT ENACTED BY THE GENERAL ASSEMBLY OF MARYLAND,

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

That the Laws of Maryland read as follows:

Article – Public Safety

14–104.2.

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

(2) "Fund" means the Local Cybersecurity Support Fund.

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

(b) (1) There is a Local Cybersecurity Support Fund.

(2) The purpose of the Fund is to:

(i) provide financial assistance to local governments to improve cybersecurity preparedness, including:

1. updating current devices and networks with the most up–to–date cybersecurity protections;

2. supporting the purchase of new hardware, software, devices, and firewalls to improve cybersecurity preparedness;

3. recruiting and hiring information technology staff focused on cybersecurity;

4. paying outside vendors for cybersecurity staff training;

5. conducting cybersecurity vulnerability assessments;

6. addressing high–risk cybersecurity vulnerabilities identified by vulnerability assessments;

7. implementing and maintaining integrators and other similar intelligence sharing infrastructure that enable connection with the Information Sharing and Analysis Center in the Department of Information Technology; and

8. supporting the security of local wastewater treatment plants, including bicounty, county, and municipal plants, by acquiring or implementing cybersecurity–related upgrades to the plants; and

(ii) assist local governments applying for federal cybersecurity preparedness grants.

(3) The Secretary shall administer the Fund.

(4) (i) The Fund is a special, nonlapsing fund that is not subject to § 7–302 of the State Finance and Procurement Article.

(ii) The State Treasurer shall hold the Fund separately, and the Comptroller shall account for the Fund.

(5) The Fund consists of:

(i) money appropriated in the State budget to the Fund;

(ii) interest earnings; and

(iii) any other money from any other source accepted for the benefit of the Fund.

(6) The Fund may be used only:

(i) to provide financial assistance to local governments to improve cybersecurity preparedness, including:

1. updating current devices and networks with the most up–to–date cybersecurity protections;

2. supporting the purchase of new hardware, software, devices, and firewalls to improve cybersecurity preparedness;

3. recruiting and hiring information technology staff focused on cybersecurity;

4. paying outside vendors for cybersecurity staff training;

5. conducting cybersecurity vulnerability assessments;

6. addressing high–risk cybersecurity vulnerabilities identified by vulnerability assessments;

7. implementing or maintaining integrators and other similar intelligence sharing infrastructure that enable connection with the Information Sharing and Analysis Center in the Department of Information Technology; and

8. supporting the security of local wastewater treatment plants, including bicounty, county, and municipal plants, by acquiring or implementing cybersecurity–related upgrades to the plants;

(ii) to assist local governments applying for federal cybersecurity

preparedness grants; and

(iii) for administrative expenses associated with providing the assistance described under item (i) of this paragraph.

(7) (i) The State Treasurer shall invest the money of the Fund in the same manner as other State money may be invested.

(ii) Any interest earnings of the Fund shall be credited to the Fund.

(8) Expenditures from the Fund may be made only in accordance with the State budget.

(c) To be eligible to receive assistance from the Fund, a local government shall:

(1) provide proof to the Department of Information Technology that the local government conducted a cybersecurity preparedness assessment in the previous 12 months; or

(2) within 12 months undergo a cybersecurity preparedness assessment provided by, in accordance with the preference of the local government:

(i) the Department of Information Technology at a cost to the local government that does not exceed the cost to the Department of Information Technology of providing the assessment; or

(ii) a vendor authorized by the Department of Information Technology to complete cybersecurity preparedness assessments.

(D) FOR FISCAL YEARS 2026 AND 2027, THE GOVERNOR MAY INCLUDE IN THE ANNUAL BUDGET BILL AN APPROPRIATION OF $10,000,000 FOR THE FUND.

Article – State Finance and Procurement

3.5–101.

(c) "Department" means the Department of Information Technology.

3.5–2A–02.

There is an Office of Security Management within the Department.

3.5–2A–03.

(e) (1) (i) There is a Director of Local Cybersecurity, who shall be appointed by the State Chief Information Security Officer.

(ii) The Director of Local Cybersecurity shall work in coordination with the Maryland Department of Emergency Management to provide technical assistance, coordinate resources, and improve cybersecurity preparedness for units of local government.

(III) THE DEPARTMENT SHALL PROVIDE SUFFICIENT INFORMATION SECURITY OFFICERS TO ASSIST THE DIRECTOR OF LOCAL CYBERSECURITY.

(2) (i) There is a Director of State Cybersecurity, who shall be appointed by the State Chief Information Security Officer.

(ii) The Director of State Cybersecurity is responsible for implementation of this section with respect to units of State government.

3.5–301.

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

(b) "Cybersecurity" means processes or capabilities wherein systems, communications, and information are protected and defended against damage, unauthorized use or modification, and exploitation.

3.5–405.

(a) This section does not apply to municipal governments.

(b) In a manner and frequency established in regulations adopted by the Department, each county government, local school system, and local health department shall in consultation with the local emergency manager, create or update a cybersecurity preparedness and response plan and complete a cybersecurity preparedness assessment.

(C) BY JULY 1, 2025, A LOCAL SCHOOL SYSTEM SHALL IMPLEMENT:

(1) MULTIFACTOR AUTHENTICATION FOR ALL SCHOOL EMPLOYEES;

(2) ENDPOINT DETECTION AND RESPONSE ON ALL SYSTEM–OWNED DEVICES ACCESSED BY EMPLOYEES; AND

(3) NETWORK MONITORING.

(D) EACH YEAR, A LOCAL SCHOOL SYSTEM SHALL REPORT IN A CYBERSECURITY ASSESSMENT REQUIRED UNDER § 3.5–407 OF THIS SUBTITLE THE PERCENTAGE OF EMPLOYEES THAT COMPLY WITH THE REQUIREMENTS OF EACH ITEM OF SUBSECTION (C) OF THIS SECTION.

3.5–407.

(a) This section does not apply to municipal governments.

(b) In a manner and frequency established in regulations adopted by the Department, each county government, local school system, and local health department shall:

(1) in consultation with the local emergency manager, create or update a cybersecurity preparedness and response plan; and

(2) complete a cybersecurity preparedness assessment.

(c) The assessment required under paragraph (b)(2) of this section may, in accordance with the preference of each county government, be performed by the Department or by a vendor authorized by the Department.

(d) (1) Each local government shall report a cybersecurity incident, including an attack on a State system being used by the local government, to the appropriate local emergency manager and the State Security Operations Center in the Department in accordance with paragraph (2) of this subsection.

(2) For the reporting of cybersecurity incidents to local emergency managers under subparagraph (i) of this paragraph, the State Chief Information Security Officer shall determine:

(i) the criteria for determining when an incident must be reported;

(ii) the manner in which to report; and

(iii) the time period within which a report must be made.

(3) The State Security Operations Center shall immediately notify the appropriate agencies of a cybersecurity incident reported under this subsection through the State Security Operations Center.

SECTION 2. AND BE IT FURTHER ENACTED, That, for fiscal years 2026 and 2027, funds from the Dedicated Purpose Account may be transferred by budget amendment, in accordance with § 7–310 of the State Finance and Procurement Article, to implement this Act.

SECTION 3. AND BE IT FURTHER ENACTED, That this Act shall take effect July 1, 2024.