SENATE BILL 907

F1, S2 5lr2152
CF 5lr3329

By: **Senator Hester**
Introduced and read first time: January 28, 2025
Assigned to: Education, Energy, and the Environment

A BILL ENTITLED

AN ACT concerning

Cybersecurity – Standards, Compliance, and Audits – Alterations

FOR the purpose of repealing the requirement that county boards of education prioritize the purchase of digital devices with certain funds; requiring each local school system to comply with, and certify compliance with, the State minimum cybersecurity standards and to conduct a cybersecurity maturity assessment every 2 years; requiring the Office of Security Management within the Department of Information Technology to annually update the State minimum cybersecurity standards; requiring the Department of Information Technology to provide a certain number of information security officers to assist local school systems with certain functions and to focus on a certain standard for a certain school year; requiring the Office of Legislative Audits within the Department of Legislative Services to refer to the State minimum cybersecurity standards when conducting certain audits; and generally relating to cybersecurity.

BY repealing and reenacting, with amendments,
Article – Education
Section 5–212
Annotated Code of Maryland
(2022 Replacement Volume and 2024 Supplement)

BY adding to
Article – Education
Section 5–213(e) and (f)
Annotated Code of Maryland
(2022 Replacement Volume and 2024 Supplement)

BY repealing and reenacting, with amendments,
Article – State Finance and Procurement
Section 3.5–101, 3.5–2A–04(b), and 3.5–405
Annotated Code of Maryland

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

(2021 Replacement Volume and 2024 Supplement)

BY repealing and reenacting, without amendments,
Article – State Finance and Procurement
Section 3.5–2A–02 and 3.5–301(a) and (c)
Annotated Code of Maryland
(2021 Replacement Volume and 2024 Supplement)

BY repealing and reenacting, with amendments,
Article – State Government
Section 2–1221
Annotated Code of Maryland
(2021 Replacement Volume and 2024 Supplement)

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

Article – Education

5–212.

(a) The target per pupil foundation amount includes costs associated with implementing the Blueprint for Maryland's Future including:

(1) Increasing salaries;

(2) Additional teachers to provide professional learning and collaborative time for teachers;

(3) Career counseling;

(4) Behavioral health;

(5) Instructional opportunities for students who are college and career ready and those who are not;

(6) Maintenance and operation of schools;

(7) Supplies and materials for teachers; and

(8) Educational technology including digital devices, broadband connectivity, **[**and**]** information technology staff**, AND CYBERSECURITY**.

(b) Schools may use funds provided under this section to provide the programs required under COMAR 13A.04.16.01.

(c) (1) **[**County boards of education and schools shall prioritize the purchase

of digital devices for using funds under subsection (a)(8) of this section.

(2)**]** Additional funds provided in the target per pupil foundation amount for educational technology are intended to supplement and not supplant existing funding provided for educational technology.

[(3)**] (2)** (i) On or before **[**November 15 each year**] AUGUST 15, 2025, AND EACH AUGUST 15 THEREAFTER**, each county board shall submit a report to the Department detailing, for the previous fiscal year:

1. The amount spent by the local school system on **[**technology disaggregated by digital devices, connectivity, and**]** information technology staff**[**; and**] DISAGGREGATED BY:**

A. FULL–TIME EMPLOYEES;

B. VENDOR–SUPPORTED STAFF OR CONTRACTORS; AND

C. DEDICATED CYBERSECURITY PROFESSIONALS BY TYPE, INCLUDING CHIEF INFORMATION SECURITY OFFICERS AND CYBERSECURITY SPECIALISTS;

2. The percentage of students, teachers, and staff with digital devices and adequate connectivity in their homes in accordance with the Federal Communications Commission standards for broadband**; AND**

3. CYBERSECURITY EXPENDITURES RELATED TO THE STATE MINIMUM CYBERSECURITY STANDARDS ESTABLISHED BY THE DEPARTMENT OF INFORMATION TECHNOLOGY.

(ii) On or before December 15 each year, the Department shall submit to the General Assembly, in accordance with § 2–1257 of the State Government Article, a compilation of the reports submitted to the Department under subparagraph (i) of this paragraph.

(iii) On or before September 1, 2021, the Department shall establish uniform reporting requirements, including definitions to ensure that consistent and comparable reports are submitted under subparagraph (i) of this paragraph.

5–213.

(E) (1) EACH COUNTY BOARD SHALL PROVIDE SUFFICIENT CYBERSECURITY STAFFING AS DETERMINED BY THE STATE CHIEF INFORMATION SECURITY OFFICER.

(2) LOCAL SCHOOL SYSTEMS MAY SHARE SERVICES, CONTRACTORS, OR REGIONAL SUPPORT FROM THE DEPARTMENT TO MEET THE REQUIREMENTS OF SUBPARAGRAPH (I) OF THIS PARAGRAPH, PROVIDED THAT EACH LOCAL SCHOOL SYSTEM ENSURES TIMELY AND ADEQUATE SUPPORT FOR CYBERSECURITY.

(F) (1) BEGINNING IN 2026, EACH LOCAL SCHOOL SYSTEM SHALL:

(I) COMPLY WITH THE STATE MINIMUM CYBERSECURITY STANDARDS; AND

(II) CONDUCT A CYBERSECURITY MATURITY ASSESSMENT EVERY 2 YEARS.

(2) ON OR BEFORE JUNE 30, 2026, AND EACH JUNE 30 EVERY 2 YEARS THEREAFTER, EACH LOCAL SCHOOL SYSTEM SHALL CERTIFY TO THE OFFICE OF SECURITY MANAGEMENT WITHIN THE DEPARTMENT OF INFORMATION TECHNOLOGY COMPLIANCE WITH THE STATE MINIMUM CYBERSECURITY STANDARDS.

Article – State Finance and Procurement

3.5–101.

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

(b) "Cloud computing" means a service that enables on–demand self–service network access to a shared pool of configurable computer resources, including data storage, analytics, commerce, streaming, e–mail, document sharing, and document editing.

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

(d) "Secretary" means the Secretary of Information Technology.

(E) "STATE MINIMUM CYBERSECURITY STANDARDS" MEANS THE STATE MINIMUM CYBERSECURITY STANDARDS ESTABLISHED BY THE DEPARTMENT OF INFORMATION TECHNOLOGY.

[(e)**] (F)** "Telecommunication" means the transmission of information, images, pictures, voice, or data by radio, video, or other electronic or impulse means.

[(f)**] (G)** "Unit of State government" means an agency or unit of the Executive Branch of State government.

3.5–2A–02.

There is an Office of Security Management within the Department.

3.5–2A–04.

(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 an entity connected to the network established under § 3.5–404 of this title that introduces 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) ANNUALLY REVIEW AND UPDATE THE STATE MINIMUM CYBERSECURITY STANDARDS; AND

(15) provide technical services, advice, and guidance to units of local government to improve cybersecurity preparedness, prevention, response, and recovery practices.

3.5–301.

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

(c) "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) THE DEPARTMENT SHALL ASSIGN AT LEAST THREE INFORMATION SECURITY OFFICERS TO SUPPORT LOCAL SCHOOL SYSTEMS WITH:

(1) COMPLIANCE WITH THE STATE MINIMUM CYBERSECURITY STANDARDS;

(2) CONDUCTING CYBERSECURITY MATURITY ASSESSMENTS EVERY 2 YEARS; AND

(3) REMEDIATION EFFORTS.

(D) ON OR BEFORE JUNE 30, 2026, AND EACH JUNE 30 EVERY 2 YEARS THEREAFTER, EACH LOCAL SCHOOL SYSTEM SHALL CERTIFY TO THE OFFICE OF SECURITY MANAGEMENT COMPLIANCE WITH THE STATE MINIMUM CYBERSECURITY STANDARDS.

Article – State Government

2–1221.

(a) A fiscal/compliance audit conducted by the Office of Legislative Audits shall include:

(1) examining financial transactions and records and internal controls;

(2) evaluating compliance with applicable laws and regulations;

(3) examining electronic data processing operations; and

(4) evaluating compliance with applicable laws and regulations relating to the acquisition of goods and services from Maryland Correctional Enterprises.

(b) A performance audit conducted by the Office of Legislative Audits may include:

(1) evaluating the efficiency, effectiveness, and economy with which resources are used;

(2) determining whether desired program results are achieved; and

(3) determining the reliability of performance measures, as defined in § 3–1001(g) of the State Finance and Procurement Article, identified in:

(i) the managing for results agency strategic plan developed under § 3–1002(c) of the State Finance and Procurement Article; or

(ii) the StateStat agency strategic plan developed under § 3–1003(d) of the State Finance and Procurement Article.

(c) The purpose of financial statement audits conducted by the Office of Legislative Audits shall be to express an opinion regarding the fairness of the presentation of a unit's financial statements.

(d) **(1)** The audits referred to in subsections (a), (b), and (c) of this section shall be conducted in accordance with generally accepted government auditing standards.

(2) FOR THE AUDITS REFERRED TO IN SUBSECTIONS (A), (B), AND (C) OF THIS SECTION, THE OFFICE OF LEGISLATIVE AUDITS SHALL BE GUIDED BY THE DEPARTMENT OF INFORMATION TECHNOLOGY'S STATE MINIMUM CYBERSECURITY STANDARDS.

(e) (1) Upon approval of the Joint Audit and Evaluation Committee, the Office

of Legislative Audits shall develop and use a rating system that is based on the results of a fiscal/compliance audit to determine an overall evaluation of a unit's financial transactions, records, and internal controls and compliance with applicable laws and regulations as a means of comparing the various units of State government.

(2) When an evaluation is issued, it shall be provided to the unit and shall be available to the Joint Audit and Evaluation Committee and the Budget Committees of the Maryland General Assembly.

SECTION 2. AND BE IT FURTHER ENACTED, That, for the 2025–2026 school year, the Department of Information Technology shall focus on Standard 6.2 Protect (PR) Controls of the State minimum cybersecurity standards.

SECTION 3. AND BE IT FURTHER ENACTED, That this Act shall take effect July 1, 2025.