Chapter 34

(House Bill 957)

AN ACT concerning

Cybersecurity – Standards and Compliance – Alterations

FOR the purpose of requiring each local school system to designate a local point of contact for certain communications, to comply with, and certify compliance with, the State minimum cybersecurity standards, and to conduct a cybersecurity maturity assessment periodically; ~~repealing the requirement that county boards of education prioritize the purchase of digital devices with certain funds;~~ requiring the Office of Security Management within the Department of Information Technology to annually review and, if necessary, update the State minimum cybersecurity standards; requiring the Department to ~~support~~ advise local school systems ~~with~~ on certain functions ~~and to focus on a certain standard for a certain school year~~; and generally relating to cybersecurity.

BY adding to
Article – Education
Section 4–148
Annotated Code of Maryland
(2025 Replacement Volume and 2025 Supplement)

~~BY repealing and reenacting, with amendments,~~
~~Article – Education~~
~~Section 5–212~~
~~Annotated Code of Maryland~~
~~(2025 Replacement Volume and 2025 Supplement)~~

BY repealing and reenacting, with amendments,
Article – State Finance and Procurement
Section 3.5–101, 3.5–2A–04(b), and 3.5–406
Annotated Code of Maryland
(2021 Replacement Volume and 2025 Supplement)

BY repealing and reenacting, without amendments,
Article – State Finance and Procurement
Section 3.5–2A–02
Annotated Code of Maryland
(2021 Replacement Volume and 2025 Supplement)

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

Article – Education

4–148.

(A) EACH ~~COUNTY BOARD~~ LOCAL SCHOOL SYSTEM SHALL:

(1) DESIGNATE A LOCAL POINT OF CONTACT FOR ALL CYBERSECURITY–RELATED COMMUNICATIONS; AND

(2) NOTIFY THE STATE CHIEF INFORMATION SECURITY OFFICER OF:

(I) THE DESIGNATION; AND

(II) ANY SUBSEQUENT UPDATE TO THE DESIGNATION.

(B) (1) BEGINNING IN 2027, EACH LOCAL SCHOOL SYSTEM SHALL:

(I) COMPLY WITH THE STATE MINIMUM CYBERSECURITY STANDARDS ESTABLISHED BY THE DEPARTMENT OF INFORMATION TECHNOLOGY; AND

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

(2) ON OR BEFORE JUNE 30, 2027, 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 ESTABLISHED BY THE DEPARTMENT OF INFORMATION TECHNOLOGY.

~~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, 2026, 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~~**]**

~~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.~~

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) (1) "Oversight of implementation" means management of the process to implement a new technology, system, or product into practice and use by a unit.

(2) "Oversight of implementation" includes:

(i) planning and preparation to implement the product or practice; and

(ii) ongoing monitoring and support of the implementation team to ensure successful execution and that the project goals are met.

(3) "Oversight of implementation" does not include:

(i) responsibility for day–to–day management of any individual projects or products; or

(ii) responsibility for implementing individual–level process requirements for a project or product.

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

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

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

[(g)**] (H)** "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, 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;

(14) ANNUALLY REVIEW AND, IF NECESSARY, UPDATE THE STATE MINIMUM CYBERSECURITY STANDARDS;

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

[(15)**] (16)** 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.

3.5–406.

(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) ~~THE DEPARTMENT'S INFORMATION SECURITY OFFICERS~~ ON REQUEST, THE DEPARTMENT SHALL ~~SUPPORT~~ ADVISE LOCAL SCHOOL SYSTEMS ~~WITH~~ ON:

~~(1)~~ (I) COMPLIANCE WITH THE STATE MINIMUM CYBERSECURITY STANDARDS;

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

~~(3)~~ **(III) REMEDIATION EFFORTS.**

(2) THE DEPARTMENT IS NOT RESPONSIBLE FOR THE SUCCESSFUL PERFORMANCE OF OR DAY–TO–DAY MANAGEMENT OF THE DUTIES OF A LOCAL SCHOOL SYSTEM DESCRIBED IN PARAGRAPH (1) OF THIS SUBSECTION.

[(d)**] (E)** (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**]** **PARAGRAPH (1) OF THIS SUBSECTION**, 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 the 2026–2027 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, 2026.

Approved by the Governor, April 14, 2026.