

# HOUSE BILL 957

S2, F1

6lr2919  
CF SB 601

---

By: **Delegates Wu, Fair, Kaiser, Rose, and Spiegel**

Introduced and read first time: February 5, 2026

Assigned to: Government, Labor, and Elections

---

## A BILL ENTITLED

1 AN ACT concerning

### **Cybersecurity – Standards and Compliance – Alterations**

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

12 BY adding to

13 Article – Education  
14 Section 4–148  
15 Annotated Code of Maryland  
16 (2025 Replacement Volume and 2025 Supplement)

17 BY repealing and reenacting, with amendments,

18 Article – Education  
19 Section 5–212  
20 Annotated Code of Maryland  
21 (2025 Replacement Volume and 2025 Supplement)

22 BY repealing and reenacting, with amendments,

23 Article – State Finance and Procurement  
24 Section 3.5–101, 3.5–2A–04(b), and 3.5–406  
25 Annotated Code of Maryland  
26 (2021 Replacement Volume and 2025 Supplement)

27 BY repealing and reenacting, without amendments,

---

EXPLANATION: CAPITALS INDICATE MATTER ADDED TO EXISTING LAW.

[Brackets] indicate matter deleted from existing law.



1                   Article – State Finance and Procurement  
2                   Section 3.5–2A–02  
3                   Annotated Code of Maryland  
4                   (2021 Replacement Volume and 2025 Supplement)

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

6   That the Laws of Maryland read as follows:

7                   **Article – Education**

8   **4–148.**

9                   **(A) EACH COUNTY BOARD SHALL:**

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

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

13                   **(I) THE DESIGNATION; AND**

14                   **(II) ANY SUBSEQUENT UPDATE TO THE DESIGNATION.**

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

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

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

21                   **(2) ON OR BEFORE JUNE 30, 2027, AND EACH JUNE 30 EVERY 2**  
22                   **YEARS THEREAFTER, EACH LOCAL SCHOOL SYSTEM SHALL CERTIFY TO THE OFFICE**  
23                   **OF SECURITY MANAGEMENT WITHIN THE DEPARTMENT OF INFORMATION**  
24                   **TECHNOLOGY COMPLIANCE WITH THE STATE MINIMUM CYBERSECURITY**  
25                   **STANDARDS ESTABLISHED BY THE DEPARTMENT OF INFORMATION TECHNOLOGY.**

26                   **5–212.**

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

29                   (1) Increasing salaries;

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

3 (3) Career counseling;

4 (4) Behavioral health;

7 (6) Maintenance and operation of schools;

8 (7) Supplies and materials for teachers; and

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

13 (c) (1) [County boards of education and schools shall prioritize the purchase  
14 of digital devices for using funds under subsection (a)(8) of this section.

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

18                    [(3)] (2)      (i)      On or before [November 15 each year] **AUGUST 15, 2026**,  
19 **AND EACH AUGUST 15 THEREAFTER**, each county board shall submit a report to the  
20 Department detailing, for the previous fiscal year:

(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

5 3.5-101.

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

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

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

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

13 (2) "Oversight of implementation" includes:

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

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

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

19 (i) responsibility for day-to-day management of any individual  
20 projects or products; or

21 (ii) responsibility for implementing individual-level process  
22 requirements for a project or product.

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

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

27           **(f) (G)**     “Telecommunication” means the transmission of information, images,  
28    pictures, voice, or data by radio, video, or other electronic or impulse means.

29 [g] (H) "Unit of State government" means an agency or unit of the Executive

1 Branch of State government.

2 3.5–2A–02.

3 There is an Office of Security Management within the Department.

4 3.5–2A–04.

5 (b) The Office shall:

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

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

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

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

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

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

21 (7) if the State Chief Information Security Officer determines that there is  
22 a cybersecurity threat caused by, affecting, or potentially affecting an entity connected to  
23 the network established under § 3.5–404 of this title that introduces or may introduce a  
24 serious risk to entities connected to the network or to the State, take or direct actions  
25 required to mitigate the threat;

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

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

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

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

7 (13) provide technical assistance to localities in mitigating and recovering  
8 from cybersecurity incidents;

11                   **[(14)] (15)** provide technical services, advice, and guidance to units of local  
12 government to improve cybersecurity preparedness, prevention, response, and recovery  
13 practices; and

14                   **[(15)] (16)** support local governments in developing a vulnerability  
15 assessment and cyber assessment, including providing local governments with the  
16 resources and information on best practices to complete the assessments.

17 3.5-406.

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

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

24 (2) complete a cybersecurity preparedness assessment.

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

(D) THE DEPARTMENT'S INFORMATION SECURITY OFFICERS SHALL SUPPORT LOCAL SCHOOL SYSTEMS WITH:

## 32 (2) CONDUCTING CYBERSECURITY MATURITY ASSESSMENTS EVERY 2

1   YEARS; AND

2                   **(3)    REMEDIATION EFFORTS.**

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

7                (2) For the reporting of cybersecurity incidents to local emergency  
8 managers under [subparagraph (i) of this paragraph] **PARAGRAPH (1) OF THIS**  
9 **SUBSECTION**, the State Chief Information Security Officer shall determine:

10                   (i) the criteria for determining when an incident must be reported;  
11                   (ii) the manner in which to report; and  
12                   (iii) the time period within which a report must be made.

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

16                SECTION 2. AND BE IT FURTHER ENACTED, That, for the 2026–2027 school  
17 year, the Department of Information Technology shall focus on Standard 6.2 Protect (PR)  
18 Controls of the State minimum cybersecurity standards.

19                SECTION 3. AND BE IT FURTHER ENACTED, That this Act shall take effect July  
20 1, 2026.