

HOUSE BILL 376

P1, S2

(5lr1418)

ENROLLED BILL

— Health and Government Operations/Education, Energy, and the Environment —

Introduced by **Chair, Health and Government Operations Committee**

Read and Examined by Proofreaders:

Proofreader.

Proofreader.

Sealed with the Great Seal and presented to the Governor, for his approval this

_____ day of _____ at _____ o'clock, _____ M.

Speaker.

CHAPTER _____

1 AN ACT concerning

2 **Maryland Cybersecurity Council – ~~Membership~~ Alterations**

3 FOR the purpose of altering the ~~membership, selection of the membership, and chair of the~~
4 ~~Maryland Cybersecurity Council~~; *selection of the membership and chair of the*
5 *Maryland Cybersecurity Council; requiring the Council, working with certain*
6 *entities, to assess and address cybersecurity threats and associated risks from*
7 *artificial intelligence and quantum computing*; and generally relating to *the*
8 Maryland Cybersecurity Council ~~membership~~.

9 BY repealing and reenacting, without amendments,
10 Article – State Government
11 Section 9–2901(b)
12 Annotated Code of Maryland
13 (2021 Replacement Volume and 2024 Supplement)

EXPLANATION: CAPITALS INDICATE MATTER ADDED TO EXISTING LAW.

[Brackets] indicate matter deleted from existing law.

Underlining indicates amendments to bill.

~~Strike out~~ indicates matter stricken from the bill by amendment or deleted from the law by amendment.

Italics indicate opposite chamber/conference committee amendments.



1 BY repealing and reenacting, with amendments,
2 Article – State Government
3 Section 9–2901(c) ~~and (f), (f), and (j)~~
4 Annotated Code of Maryland
5 (2021 Replacement Volume and 2024 Supplement)

6 BY repealing
7 Article – State Government
8 Section 9–2901(g)
9 Annotated Code of Maryland
10 (2021 Replacement Volume and 2024 Supplement)

11 BY adding to
12 Article – State Government
13 Section 9–2901(g)
14 Annotated Code of Maryland
15 (2021 Replacement Volume and 2024 Supplement)

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

18 **Article – State Government**

19 9–2901.

20 (b) There is a Maryland Cybersecurity Council.

21 (c) The Council consists of the following members:

22 (1) the Attorney General, or the Attorney General’s designee;

23 (2) the Secretary of Information Technology, or the Secretary’s designee;

24 (3) the Secretary of State Police, or the Secretary’s designee;

25 (4) the Secretary of Commerce, or the Secretary’s designee;

26 (5) the Adjutant General, or the Adjutant General’s designee;

27 (6) the State Administrator of Elections, or the State Administrator’s
28 designee;

29 (7) the Executive Director of the Governor’s Office of Homeland Security,
30 or the Executive Director’s designee;

31 (8) the Director of the Maryland Coordination and Analysis Center, or the
32 Director’s designee;

1 (9) the Secretary of Emergency Management, or the Secretary's designee;

2 (10) THE PEOPLE'S COUNSEL, OR THE DESIGNEE OF THE PEOPLE'S
3 COUNSEL;

4 (11) the Chief Executive Officer of the Maryland Technology Development
5 Corporation, or the Chief Executive Officer's designee;

6 ~~(11)~~ (12) the Chair of the Tech Council of Maryland, or the Chair's
7 designee;

8 ~~(12) THE EXECUTIVE DIRECTOR OF THE CYBERSECURITY~~
9 ~~ASSOCIATION, INC., OR THE EXECUTIVE DIRECTOR'S DESIGNEE;~~

10 ~~(12)~~ (13) the President of the Fort Meade Alliance, or the President's
11 designee;

12 ~~(13)~~ (14) the President of the Army Alliance, or the President's designee;
13 ~~and~~

14 ~~(14)~~ (15) ~~the following members appointed by the [Attorney General]~~
15 ~~GOVERNOR;~~

16 ~~(i)~~ (i) ~~five~~ **FOUR** representatives of cybersecurity companies located in
17 the State, with at least three representing cybersecurity companies with 50 or fewer
18 employees, DESIGNATED BY THE CYBERSECURITY ASSOCIATION OF MARYLAND;

19 ~~(ii)~~ (ii) ~~four representatives from statewide or regional business~~
20 ~~associations;~~

21 (16) THE CHIEF EXECUTIVE OFFICER OF THE MARYLAND CHAMBER OF
22 COMMERCE, OR THE CHIEF EXECUTIVE OFFICER'S DESIGNEE;

23 (17) THE EXECUTIVE DIRECTOR OF THE CYBERSECURITY
24 ASSOCIATION OF MARYLAND, OR THE EXECUTIVE DIRECTOR'S DESIGNEE;

25 ~~(iii)~~ (18) ~~up to ten~~ **NINE** representatives from institutions of higher
26 education located in the State WITH EXPERTISE IN CYBERSECURITY, WITH AT LEAST
27 FOUR REPRESENTATIVES WITH EXPERTISE IN ARTIFICIAL INTELLIGENCE AND
28 QUANTUM COMPUTING, INCLUDING:

29 (I) THE PRESIDENT, OR THE PRESIDENT'S DESIGNEE, OF:

30 1. BOWIE STATE UNIVERSITY;

- 1 **2. *JOHNS HOPKINS UNIVERSITY;***
- 2 **3. *MORGAN STATE UNIVERSITY;***
- 3 **4. *THE UNIVERSITY OF MARYLAND, BALTIMORE***
4 **CAMPUS;**
- 5 **5. *THE UNIVERSITY OF MARYLAND, BALTIMORE***
6 **COUNTY; AND**
- 7 **6. *THE UNIVERSITY OF MARYLAND, COLLEGE PARK***
8 **CAMPUS;**

9 **(II) *THE DEAN OF THE UNIVERSITY OF MARYLAND GLOBAL***
10 **CAMPUS SCHOOL OF CYBERSECURITY AND INFORMATION TECHNOLOGY, OR THE**
11 **DEAN'S DESIGNEE; AND**

12 **(III) *TWO ADDITIONAL REPRESENTATIVES DESIGNATED BY THE***
13 **CHANCELLOR OF THE UNIVERSITY SYSTEM OF MARYLAND;**

14 ~~(iv) one representative of a crime victims organization;~~

15 ~~(v) four representatives from industries that may be susceptible to~~
16 ~~attacks on cybersecurity, including at least one representative of a bank, whether or not~~
17 ~~State chartered, that has a branch in the State;~~

18 ~~(vi) two representatives of organizations that have expertise in~~
19 ~~electronic health care records; and~~

20 **(19) *THE DIRECTOR OF CASH CAMPAIGN OF MARYLAND, OR THE***
21 **DIRECTOR'S DESIGNEE;**

22 **(20) *THE EXECUTIVE DIRECTOR OF ECONOMIC ACTION MARYLAND,***
23 **OR THE EXECUTIVE DIRECTOR'S DESIGNEE;**

24 **(21) *ONE BANK CHIEF INFORMATION SECURITY OFFICER, DESIGNATED***
25 **BY THE MARYLAND BANKERS ASSOCIATION;**

26 **(22) *ONE HOSPITAL CHIEF INFORMATION SECURITY OFFICER,***
27 **DESIGNATED BY THE MARYLAND HOSPITAL ASSOCIATION;**

28 **(23) *ONE WATER SYSTEMS CHIEF INFORMATION SECURITY OFFICER***
29 **WHO WORKS FOR A WATER SYSTEM LOCATED IN THE STATE, DESIGNATED BY THE**
30 **NATIONAL ASSOCIATION OF WATER COMPANIES;**

1 (24) ONE ELECTRIC COMPANY CHIEF INFORMATION SECURITY OFFICER
 2 WHO WORKS IN THE STATE FOR AN ELECTRIC COMPANY SERVING CUSTOMERS IN THE
 3 STATE, DESIGNATED BY THE EDISON ELECTRIC INSTITUTE;

4 (25) THE EXECUTIVE DIRECTOR OF THE ELECTRONIC PRIVACY
 5 INFORMATION CENTER, OR THE EXECUTIVE DIRECTOR'S DESIGNEE;

6 (26) THE EXECUTIVE DIRECTOR OF THE CENTER FOR DEMOCRACY
 7 AND TECHNOLOGY, OR THE EXECUTIVE DIRECTOR'S DESIGNEE;

8 (27) THE CHIEF EXECUTIVE OFFICER OF THE TECHNOLOGY
 9 ADVANCEMENT CENTER, OR THE CHIEF EXECUTIVE OFFICER'S DESIGNEE;

10 (28) THE DIRECTOR OF THE CENTER FOR GOVERNANCE OF
 11 TECHNOLOGY AND SYSTEMS, OR THE DIRECTOR'S DESIGNEE; AND

12 ~~(vii)~~ (29) any other stakeholder that the [Attorney General]
 13 ~~GOVERNOR~~ CHAIR determines appropriate.

14 (f) The [Attorney General] ~~GOVERNOR~~ CHAIR also shall invite, as appropriate,
 15 the following representatives of federal agencies to serve on the Council:

16 (1) the Director of the National Security Agency, or the Director's designee;

17 (2) the Secretary of Homeland Security, or the Secretary's designee;

18 (3) the Director of the Defense Information Systems Agency, or the
 19 Director's designee;

20 (4) THE DIRECTOR OF THE NATIONAL INSTITUTE FOR SCIENCE AND
 21 TECHNOLOGY, OR THE DIRECTOR'S DESIGNEE;

22 (5) the Director of the Intelligence Advanced Research Projects Activity, or
 23 the Director's designee; and

24 ~~(5)~~ (6) any other federal agency that the ~~Attorney General~~ CHAIR
 25 determines appropriate.

26 [(g) The Attorney General, or the Attorney General's designee, shall chair the
 27 Council.]

28 (G) (1) BEGINNING SUBJECT TO PARAGRAPH (2) OF THIS SUBSECTION,
 29 BEGINNING OCTOBER 1, 2025, AND EVERY 2 YEARS THEREAFTER, THE COUNCIL

1 SHALL ELECT A CHAIR AND VICE CHAIR FROM AMONG THE MEMBERS OF THE
2 COUNCIL.

3 (2) ONE SHALL BE A STATE EMPLOYEE AND ONE SHALL BE A
4 NON-STATE EMPLOYEE.

5 (j) The Council shall work with the National Institute of Standards and
6 Technology and other federal agencies, private sector businesses, NONPROFITS, and private
7 cybersecurity experts to ASSESS AND ADDRESS CYBERSECURITY THREATS AND
8 ASSOCIATED RISKS FROM ARTIFICIAL INTELLIGENCE AND QUANTUM COMPUTING TO:

9 (1) for critical infrastructure [not covered by federal law or the Executive
10 Order], review and conduct risk assessments to determine which local infrastructure sectors
11 are at the greatest risk of cyber attacks and need the most enhanced cybersecurity measures;

12 (2) use federal guidance to identify categories of critical infrastructure as
13 critical cyber infrastructure if cyber damage or unauthorized cyber access to the
14 infrastructure could reasonably result in catastrophic consequences, including:

15 (i) interruption in the provision of energy, water, transportation,
16 emergency services, food, or other life-sustaining services sufficient to cause a mass casualty
17 event or mass evacuations;

18 (ii) catastrophic economic damage; or

19 (iii) severe degradation of State or national security;

20 (3) assist infrastructure entities that are not covered by the Executive Order
21 in complying with federal cybersecurity guidance;

22 (4) assist private sector cybersecurity businesses in adopting, adapting, and
23 implementing the National Institute of Standards and Technology cybersecurity framework
24 of standards and practices;

25 (5) examine inconsistencies between State and federal laws regarding
26 cybersecurity;

27 (6) recommend a comprehensive State strategic plan to ensure a coordinated
28 and adaptable response to and recovery from cybersecurity attacks; [and]

29 (7) ADDRESS SENSITIVE PRIVACY INTERESTS OF STATE RESIDENTS
30 RELATED TO CYBERSECURITY AND ASSOCIATED RISKS;

31 (8) ADDRESS EMERGING THREATS POSED BY ARTIFICIAL
32 INTELLIGENCE, INCLUDING:

1 **(I) ADVERSARIAL ARTIFICIAL INTELLIGENCE;**

2 **(II) CYBER ATTACKS;**

3 **(III) DEEPFAKE TECHNOLOGIES;**

4 **(IV) UNETHICAL USE; AND**

5 **(V) FRAUD; AND**

6 **[(7)] (9) recommend any legislative changes considered necessary by the**
7 **Council to address cybersecurity issues.**

8 **SECTION 2. AND BE IT FURTHER ENACTED, That it is the intent of the General**
9 **Assembly that the Maryland Cybersecurity Council reviews and adjusts its subcommittee**
10 **structure, if necessary, and implements appropriate bylaws of operation consistent with**
11 **State law by December 1, 2025.**

12 SECTION ~~2.~~ 3. AND BE IT FURTHER ENACTED, That this Act shall take effect
13 October 1, 2025.

Approved:

Governor.

Speaker of the House of Delegates.

President of the Senate.