Chapter 627

(House Bill 376)

AN ACT concerning

Maryland Cybersecurity Council – ~~Membership –~~ Alterations

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

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

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

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

BY adding to
Article – State Government
Section 9–2901(g)
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 – State Government

9–2901.

(b) There is a Maryland Cybersecurity Council.

(c) The Council consists of the following members:

(1) the Attorney General, or the Attorney General's designee;

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

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

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

(5) the Adjutant General, or the Adjutant General's designee;

(6) the State Administrator of Elections, or the State Administrator's designee;

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

1. BOWIE STATE UNIVERSITY;

2. JOHNS HOPKINS UNIVERSITY;

3. MORGAN STATE UNIVERSITY;

4. THE UNIVERSITY OF MARYLAND, BALTIMORE CAMPUS;

5. THE UNIVERSITY OF MARYLAND, BALTIMORE COUNTY; AND

6. THE UNIVERSITY OF MARYLAND, COLLEGE PARK CAMPUS;

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

(G) ***(1)*** ~~**BEGINNING**~~ ***SUBJECT TO PARAGRAPH (2) OF THIS SUBSECTION, BEGINNING*** **OCTOBER 1, 2025, AND EVERY 2 YEARS THEREAFTER, THE COUNCIL SHALL ELECT A CHAIR** ***AND VICE CHAIR*** **FROM AMONG THE MEMBERS OF THE COUNCIL.**

(2) ONE SHALL BE A STATE EMPLOYEE AND ONE SHALL BE A NON–STATE EMPLOYEE.

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

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

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

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

(ii) catastrophic economic damage; or

(iii) severe degradation of State or national security;

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

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

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

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

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

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

(I) ADVERSARIAL ARTIFICIAL INTELLIGENCE;

(II) CYBER ATTACKS;

(III) DEEPFAKE TECHNOLOGIES;

(IV) UNETHICAL USE; AND

(V) FRAUD; AND

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

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

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

Approved by the Governor, May 20, 2025.