HOUSE BILL 1306

P1 1lr2898

By: **Delegate Lisanti**
Introduced and read first time: February 8, 2021
Assigned to: Ways and Means

A BILL ENTITLED

AN ACT concerning

Maryland Cybersecurity Council – Election Security and High–Speed Internet Access

FOR the purpose of altering the duties of the Maryland Cybersecurity Council to include monitoring and evaluating certain election security measures and high–speed Internet access in the State; requiring the Council to make certain recommendations concerning election security and high–speed Internet access; and generally relating to the Maryland Cybersecurity Council.

BY repealing and reenacting, with amendments,
Article – State Government
Section 9–2901
Annotated Code of Maryland
(2014 Replacement Volume and 2020 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.

(a) (1) In this subtitle the following words have the meanings indicated.

(2) "Council" means the Maryland Cybersecurity Council.

(3) "Executive Order" means Executive Order 13636 of the President of the United States.

(b) There is a Maryland Cybersecurity Council.

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

(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 Executive Director of the Maryland Emergency Management Agency, or the Executive Director's designee;

(10) the Executive Director of the Maryland Technology Development Corporation, or the Executive Director's designee;

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

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

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

(14) the following members appointed by the Attorney General:

(i) five representatives of cybersecurity companies located in the State, with at least three representing cybersecurity companies with 50 or fewer employees;

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

(iii) up to ten representatives from institutions of higher education located in the State;

(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

(vii) any other stakeholder that the Attorney General determines appropriate.

(d) The President of the Senate may appoint up to two members of the Senate to serve on the Council.

(e) The Speaker of the House of Delegates may appoint up to two members of the House to serve on the Council.

(f) The Attorney General 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 Intelligence Advanced Research Projects Activity, or the Director's designee; and

(5) any other federal agency that the Attorney General determines appropriate.

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

(h) The University of Maryland Global Campus shall provide staff for the Council.

(i) A member of the Council:

(1) may not receive compensation as a member of the Council; but

(2) is entitled to reimbursement for expenses under the Standard State Travel Regulations, as provided in the State budget.

(j) The Council shall work with the National Institute of Standards and Technology and other federal agencies, private sector businesses, and private cybersecurity experts 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 cyberattacks 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) MONITOR AND EVALUATE THE EFFECTIVENESS OF MEASURES TAKEN TO ENSURE ELECTION SECURITY IN THE STATE;

(8) MONITOR AND EVALUATE THE STATUS OF HIGH–SPEED INTERNET ACCESS IN THE STATE; AND

[(7)**] (9)** recommend any legislative changes considered necessary by the Council to address cybersecurity issues**, ELECTION SECURITY, AND HIGH–SPEED INTERNET ACCESS IN THE STATE**.

(k) Beginning July 1, 2017, and every 2 years thereafter, the Council shall submit a report of its activities to the General Assembly in accordance with § 2–1257 of this article.

SECTION 2. AND BE IT FURTHER ENACTED, That this Act shall take effect October 1, 2021.