SENATE BILL 249

P1 4lr1734
SB 494/13 – FIN CF 4lr1738

By: **Senators Pugh, Astle, Conway, Currie, Feldman, Forehand, Jones–Rodwell, Kelley, King, Montgomery, Muse, and Stone**
Introduced and read first time: January 17, 2014
Assigned to: Finance

A BILL ENTITLED

AN ACT concerning

Commission on Maryland Cybersecurity Innovation and Excellence – Duties

FOR the purpose of requiring the Commission on Maryland Cybersecurity Innovation and Excellence to study and develop certain strategies and recommendations for advancing telemedicine technologies and use; and generally relating to the duties of the Commission on Maryland Cybersecurity Innovation and Excellence.

BY repealing and reenacting, with amendments,
Article – State Government
Section 9–2901
Annotated Code of Maryland
(2009 Replacement Volume and 2013 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) There is a Commission on Maryland Cybersecurity Innovation and Excellence.

(b) (1) The Commission consists of the following members:

(i) one member of the Senate of Maryland, appointed by the President of the Senate;

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

(ii) one member of the House of Delegates, appointed by the Speaker of the House;

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

(iv) the Secretary of Business and Economic Development, or the Secretary's designee;

(v) the Secretary of the Department of Labor, Licensing, and Regulation, or the Secretary's designee;

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

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

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

(ix) the following members appointed by the Governor:

1. five representatives of cybersecurity companies located in the State, with at least three representing cybersecurity companies with 50 employees or less;

2. three representatives from statewide or regional business associations;

3. four representatives from institutions of higher education located in the State;

4. one representative of a crime victims organization;

5. three representatives from industries that may be susceptible to attacks on cybersecurity; and

6. one representative of an organization that has expertise in electronic health care records.

(2) The Governor also shall invite the following representatives of federal agencies to serve on the Commission:

(i) the Director of the National Institute for Standards and Technology, or the Director's designee;

(ii) the Secretary of Defense, or the Secretary's designee;

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

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

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

(vi) the Director of the Intelligence Advanced Research Projects Activity, or the Director's designee.

(c) The members appointed by the Presiding Officers of the General Assembly shall cochair the Commission.

(d) The University of Maryland University College shall provide staff for the Commission.

(e) A member of the Commission:

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

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

(f) The purpose of the Commission is to provide a road map for making the State the epicenter of cybersecurity innovation and excellence.

(g) The Commission shall:

(1) conduct a comprehensive review of and identify any inconsistencies in:

(i) State and federal cybersecurity laws; and

(ii) policies, standards, and best practices for ensuring the security of computer systems and networks used by educational institutions and State government and other organizations that work with health care records, personal identification information, public safety, and public service and utilities;

(2) conduct a comprehensive review of the State's role in promoting cyber innovation;

(3) identify any federal preemption issues relating to cybersecurity;

(4) provide recommendations for:

(i) a comprehensive State framework and strategic plan for cybersecurity innovation and excellence;

(ii) a comprehensive State strategic plan to ensure a coordinated and adaptable response to and recovery from attacks on cybersecurity;

(iii) coordinated and unified policies to clarify the roles and responsibilities of State units regarding cybersecurity;

(iv) growth opportunities and economic development strategies and action plans; and

(v) strategies that can be used to coordinate State and federal resources to attract private sector investment and job creation in cybersecurity;

(5) make recommendations regarding:

(i) methods the State can use to increase cybersecurity innovation by:

1. promoting public and private partnerships, research and development, and workforce training, education, and development;

2. promoting science, technology, engineering, and mathematics courses in all levels of education;

3. helping companies transfer research to product;

4. protecting intellectual properties; and

5. leveraging federal funds for research, development, and commercialization;

(ii) methods that the State can use to promote collaboration and coordination among cybersecurity companies and among institutions of higher education located in the State;

(iii) a unit of State government that is suitable to run a pilot program regarding cybersecurity; and

(iv) the designation of a cybersecurity policy official that would be responsible for coordinating the State's cybersecurity policies, strategies, and activities**; AND**

(6) STUDY AND DEVELOP STRATEGIES AND RECOMMENDATIONS FOR ADVANCING TELEMEDICINE TECHNOLOGIES AND USE, INCLUDING:

(I) METHODS OF SUPPORTING INNOVATION, DEVELOPMENT, AND INVESTMENT IN THE EMERGING TECHNOLOGY;

(II) THE PROTECTION OF DATABASES IN THE USE OF TELEMEDICINE; AND

(III) ANY OTHER ISSUES RELATING TO ADVANCING AND SUPPORTING TELEMEDICINE TECHNOLOGIES AND USE THAT THE COMMISSION CONSIDERS APPROPRIATE.

(h) On or before January 1, 2012, the Commission shall submit an interim report of its findings and recommendations, including recommended legislation, to the Governor and, in accordance with § 2–1246 of this article, the General Assembly.

(i) On or before September 1, 2014, the Commission shall submit a final report of its findings and recommendations, including recommended legislation, to the Governor and, in accordance with § 2–1246 of this article, the General Assembly.

SECTION 2. AND BE IT FURTHER ENACTED, That this Act shall take effect July 1, 2014.