

HOUSE BILL 808

P1
HB 937/13 – ECM

4r1738
CF SB 249

By: **Delegates Lee, Carr, Conway, Cullison, Gutierrez, Howard, A. Kelly, McComas, Rudolph, and Sophocleus**

Introduced and read first time: February 3, 2014

Assigned to: Economic Matters

A BILL ENTITLED

1 AN ACT concerning

2 **Commission on Maryland Cybersecurity Innovation and Excellence – Duties**

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

8 BY repealing and reenacting, with amendments,
9 Article – State Government
10 Section 9–2901
11 Annotated Code of Maryland
12 (2009 Replacement Volume and 2013 Supplement)

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

15 **Article – State Government**

16 9–2901.

17 (a) There is a Commission on Maryland Cybersecurity Innovation and
18 Excellence.

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

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

EXPLANATION: CAPITALS INDICATE MATTER ADDED TO EXISTING LAW.

[Brackets] indicate matter deleted from existing law.



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

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

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

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

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

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

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

15 (ix) the following members appointed by the Governor:

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

19 2. three representatives from statewide or regional
20 business associations;

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

23 4. one representative of a crime victims organization;

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

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

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

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

- 1 (ii) the Secretary of Defense, or the Secretary's designee;
- 2 (iii) the Director of the National Security Agency, or the
3 Director's designee;
- 4 (iv) the Secretary of Homeland Security, or the Secretary's
5 designee;
- 6 (v) the Director of the Defense Information Systems Agency, or
7 the Director's designee; and
- 8 (vi) the Director of the Intelligence Advanced Research Projects
9 Activity, or the Director's designee.

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

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

14 (e) A member of the Commission:

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

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

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

20 (g) The Commission shall:

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

23 (i) State and federal cybersecurity laws; and

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

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

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

1 (4) provide recommendations for:

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

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

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

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

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

12 (5) make recommendations regarding:

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

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

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

19 3. helping companies transfer research to product;

20 4. protecting intellectual properties; and

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

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

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

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

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

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

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

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

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

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

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