SENATE BILL 692

S2, P1 4lr2434
CF 4lr3009

By: **Senators Jennings, Hershey, Hester, Simonaire, and Watson**
Introduced and read first time: January 29, 2024
Assigned to: Education, Energy, and the Environment

A BILL ENTITLED

AN ACT concerning

Cybersecurity – Workgroup to Study Data Security – Establishment

FOR the purpose of establishing the Workgroup to Study Data Security; and generally relating to the Workgroup to Study Data Security.

Preamble

WHEREAS, The world is digital and state agencies, local governments, and organizations of all types hold vast amounts of valuable data, which continues to be one of the world's most valuable assets; and

WHEREAS, Continued attacks from cyber threats and adversaries successfully breach government technology systems, steal valuable data, shut down organizations with ransomware, and exploit known and unknown vulnerabilities, all on an unprecedented scale; and

WHEREAS, With over 3,600 Data Breach Notices filed with the Office of the Attorney General in the past 3 years, representing a 700% increase over 10 years, attackers are more active than ever; and

WHEREAS, In this era of global technological transformation and data security risk, it is imperative for the State to respond; and

WHEREAS, Organizations must transform their cybersecurity strategies to ensure a data–first approach to security that keeps data secure; and

WHEREAS, Organizations must continuously assess their data security, identify potential risks and vulnerabilities, implement security controls to mitigate those risks and vulnerabilities, monitor for threats, and update their security posture; and

WHEREAS, Malicious actors are costing the State and its taxpayers millions of

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

dollars in damages through attacks on State agencies, local governments, and school systems, particularly through the use of ransomware; and

WHEREAS, In 2019, a city in Maryland suffered over $18 million of damage from a ransomware attack; and

WHEREAS, In November of 2020, at the peak of the COVID–19 pandemic, a Maryland school district halted virtual learning for more than 100,000 students due to a ransomware attack; and

WHEREAS, In 2020 and 2021, a large Maryland school district inadvertently exposed the sensitive data of more than 2,500 employees; and

WHEREAS, In 2022, a State agency suffered a ransomware attack that impacted health services during the COVID–19 pandemic; and

WHEREAS, In 2023, a large Maryland university, health care system, county government, and State agency were all impacted by a widespread zero–day attack from a vulnerability in its MOVEit software, exposing the sensitive data of thousands of Maryland citizens; and

WHEREAS, Organizations that have suffered or are under threat of cybersecurity attacks must implement data security standards to limit the potential damage of attacks, ensure that data is secure, implement sound data security principles, limit internal access to data, and develop proactive detection and response capabilities; now, therefore,

SECTION 1. BE IT ENACTED BY THE GENERAL ASSEMBLY OF MARYLAND, That:

(a) There is a Workgroup to Study Data Security.

(b) The Workgroup consists of the following members:

(1) one member of the Senate of Maryland who is a member of the Joint Committee on Cybersecurity, Information Technology, and Biotechnology, appointed by the President of the Senate;

(2) one member of the House of Delegates who is a member of the Joint Committee on Cybersecurity, Information Technology, and Biotechnology, appointed by the Speaker of the House;

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

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

(5) the Director of Local Cybersecurity in the Office of Security Management in the Department of Information Technology;

(6) the Chief Information Security Officer in the Office of Security Management in the Department of Information Technology;

(7) the State Chief Data Officer;

(8) the State Chief Privacy Officer;

(9) one representative of the Maryland Association of Counties, designated by the President of the Association;

(10) one representative of the Maryland Municipal League, designated by the President of the League;

(11) one representative of the Maryland Association of Community Colleges, designated by the Executive Director of the Association;

(12) one representative of the Maryland Independent College and University Association, designated by the Executive Director of the Association;

(13) one representative of the University System of Maryland, designated by the Chancellor;

(14) one representative of the Cybersecurity Association of Maryland, designated by the Executive Director of the Association;

(15) one representative of the Maryland Cybersecurity Council, designated by the Attorney General; and

(16) four representatives of private cybersecurity companies currently in good standing with the State Department of Assessments and Taxation, designated by the Executive Director of the Cybersecurity Association of Maryland.

(c) The President of the Senate and the Speaker of the House shall jointly designate the chair and vice chair of the Workgroup from among the members of the Workgroup appointed by the President and the Speaker.

(d) The Office of the Governor shall provide staff for the Workgroup.

(e) A member of the Workgroup:

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

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

(f) The Workgroup shall:

(1) examine data protection standards that have been proposed or adopted in other states and used by governmental entities;

(2) identify existing standards that would be best assimilated by State agencies; and

(3) develop recommendations on, and assess the fiscal impact of:

(i) data protection standards for State and local government agencies to adopt and implement;

(ii) data inventory practices by State and local government agencies;

(iii) implementation of least privilege access policies;

(iv) user access auditing policies;

(v) threat detection and response practices; and

(vi) policies around notifying citizens of data breaches.

(g) Funds appropriated to the Dedicated Purpose Account established under § 7–310 of the State Finance and Procurement Article for cybersecurity purposes may be used to support the Workgroup's activities.

(h) On or before December 1, 2024, the Workgroup shall submit an interim report of its findings and recommendations to the Governor and, in accordance with § 2–1257 of the State Government Article, the General Assembly.

(i) On or before June 30, 2025, the Workgroup shall submit a final report of its findings and recommendations to the Governor and, in accordance with § 2–1257 of the State Government Article, the General Assembly.

SECTION 2. AND BE IT FURTHER ENACTED, That this Act shall take effect July 1, 2024. It shall remain effective for a period of 2 years and, at the end of June 30, 2026, this Act, with no further action required by the General Assembly, shall be abrogated and of no further force and effect.