Department of Legislative Services

Maryland General Assembly
2024 Session

FISCAL AND POLICY NOTE
First Reader

Senate Bill 692 (Senator Jennings, *et al.*)
Education, Energy, and the Environment

Cybersecurity - Workgroup to Study Data Security - Establishment

This bill establishes the Workgroup to Study Data Security staffed by the Office of the Governor to examine data protection standards in other states and identify existing standards for State agencies. Funds appropriated to the Dedicated Purpose Account (DPA) for cybersecurity purposes may be used to support the workgroup's activities. By December 1, 2024, the workgroup must submit an interim report of its findings and recommendations to the Governor and General Assembly, and by June 30, 2025, the workgroup must submit a final report of its findings and recommendations to the Governor and General Assembly. **The bill takes effect July 1, 2024, and terminates June 30, 2026.**

Fiscal Summary

State Effect: The Office of the Governor can staff the workgroup using existing budgeted resources. Reimbursements for workgroup members are assumed to be minimal and absorbable within existing budgeted resources. Revenues are not affected.

Local Effect: The bill does not directly affect local government operations or finances.

Small Business Effect: Minimal or none.

Analysis

Bill Summary: The workgroup must (1) examine data protection standards that have been proposed or adopted in other states and used by governments; (2) identify existing standards that would be best assimilated by State agencies; and (3) develop recommendations on, and assess the fiscal impact of, specified cybersecurity issues.

A member of the workgroup may not receive compensation as a member of the workgroup but is entitled to reimbursement for expenses as provided in the State budget.

Current Law:

Data Protection by State Agencies and Local Governments

Generally, a unit of State or local government (except for the Legislative and Judicial branches of State government) that collects an individual's personal information must implement and maintain reasonable security procedures and practices appropriate to the nature of the information collected and the nature of the unit and its operations. Similarly, a unit that uses a nonaffiliated third party as a service provider (and discloses personal information about an individual) must require that the third party implement and maintain reasonable security procedures and practices.

"Reasonable security procedures and practices" means data security procedures and practices developed, in good faith, and set forth in a written information security policy. "Personal information" means an individual's first name or first initial and last name, personal mark, or unique biometric or genetic print or image, in combination with one or more of the following data elements:

- a Social Security number;
- a driver's license number, State identification card number, or other individual identification number issued by a unit of State government;
- a passport number or other identification number issued by the United States government;
- an individual Taxpayer Identification Number; or
- a financial or other account number, credit card number, or credit card number that (in combination with a security code, access code, or password) would permit access to an individual's account.

Personal information does not include a voter registration number.

More stringent personal information security requirements apply for institutions of higher education, effective October 1, 2024, pursuant to the requirements of Chapter 429 of 2020.

Cybersecurity and Dedicated Purpose Account Funding

Chapters 241, 242, and 243 of 2022 expanded and enhanced the State's regulatory framework for State and local government cybersecurity. Among other things, the Acts codified the Maryland Cyber Defense Initiative (which codified the Office of Security

Management (OSM) within the Department of Information Technology (DoIT)) and the Maryland Cybersecurity Coordinating Council and expanded the responsibilities of OSM and the council. Under the acts, OSM must develop and maintain information technology (IT) security policies, standards, and guidance documents, consistent with best practices developed by the National Institute of Standards and Technology.

The Acts also required the Governor to include in the annual budget bill for fiscal 2024 an appropriation of at least 20% of the aggregated amount appropriated for IT and cybersecurity resources in the annual budget bill for fiscal 2023. The fiscal 2024 budget as passed by the General Assembly included $152.0 million for the DPA, which is one of four accounts that make up the State Reserve Fund, to meet the mandated appropriations required for Chapters 241, 242, and 243. DoIT also processed a fiscal 2023 budget amendment to transfer $94.0 million from the DPA for remediation of State and local governments' cybersecurity.

Additional Information

Recent Prior Introductions: Similar legislation has not been introduced within the last three years.

Designated Cross File: None.

Information Source(s): Department of Information Technology; Maryland Department of Emergency Management; Maryland Municipal League; Governor's Office; University System of Maryland; Maryland Independent College and University Association; Department of Budget and Management; Department of Legislative Services

Fiscal Note History: First Reader - February 27, 2024
km/mcr

Analysis by: Richard L. Duncan

Direct Inquiries to:
(410) 946-5510
(301) 970-5510