BRIAN E. FROSH
Attorney General

ELIZABETH F. HARRIS
Chief Deputy Attorney General

CAROLYN QUATTROCKI
Deputy Attorney General

STATE OF MARYLAND
OFFICE OF THE ATTORNEY GENERAL

FACSIMILE NO.

WRITER'S DIRECT DIAL NO.
410-576-6584

March 23, 2021

TO: The Honorable Paul G. Pinsky
Chair, Education, Health, and Environmental Affairs Committee

FROM: The Office of the Attorney General

RE: SB 917 – Department of Information Technology - Status of Information Technology and Cybersecurity in State and Local Agencies – **Letter of Support**

The Office of Attorney General urges this Committee to favorably report SB 917. If passed, the bill will take effect on October 1, 2021. The legislation requires:

- By September 1 of each year, each unit of the State government shall report the current and previous fiscal years': (a) number of IT staffing positions, (b) budget broken down into "services, equipment, applications, personnel, software licensing, development, network projects, and maintenance," (c) modernization projects, (d) initiatives to test and improve security of systems and data, (e) investments to improve provision of services, and (f) plans for future fiscal years to achieve its IT goals; and
- By December 31 of each year, DoIT shall compile, analyze the information, and provide a report to each unit of the State government and the General Assembly. The report shall be broken down into unit, fiscal year, and the categories identified above. Also, the report shall include best practices recommendations to improve security and reduce costs.

Senate Bill 917 better positions DoIT to exercise an enterprise-wide cybersecurity risk management role within the State government. Unlike current law that limits DoIT's access to agencies' assets, budgets, plans, and practices,[1] SB 917 requires agencies to report this information to DoIT. Increased access to information would allow DoIT to better assist agencies

[1] *See, e.g.*, Md. Exec. Order No. 01.01.2017.22. (Oct. 5, 2017), https://content.govdelivery.com/attachments/MDGOV/2017/10/05/file_attachments/891772/Executive%2BOrder%2B01.01.2017.22.pdf (limiting access to key information about agency's cybersecurity so risk was assessed based on voluntary responses of selected agencies).

through identifying and reducing their cybersecurity risks, and advising to safely protect sensitive personal and business information.

Furthermore, better access to information will allow DoIT to make recommendations to reduce IT costs because DoIT can eliminate unnecessary duplicate protections and exploit economies of scale. For example, DoIT may recommend the most cost-effective software platforms, tools, and contracts for various IT services to state agencies.

Senate Bill 917 is consistent in part with a recommendation of the Maryland Cybersecurity Council ("Council"). The Council's last two biennial activities reports recommended to include the NIST Cybersecurity Framework in the Statewide IT Master Plan.[2] Like other recognized cybersecurity frameworks, the NIST framework emphasizes visibility into organizational IT-related assets, budgets, plans, and security practices as a prerequisite for an effective enterprise cybersecurity governance and risk management.[3]

For the foregoing reasons, the Office of the Attorney General urges a favorable report of the Senate Bill 917.

cc: Members of the Education, Health, and Environmental Affairs Committee

[2] *See generally* MD. CYBERSECURITY COUNCIL, MARYLAND CYBERSECURITY ACTIVITIES REPORT 8, 12 (July 1, 2017), https://www.umgc.edu/documents/upload/maryland-cybersecurity-council-biennial-report-2015-2017.pdf; *see also* MD. CYBERSECURITY COUNCIL, MARYLAND CYBERSECURITY ACTIVITIES REPORT 30 (July 1, 2019), https://www.umgc.edu/documents/upload/maryland-cybersecurity-council-activities-report-2017-2019.pdf.

[3] *See generally* NAT. INST. OF STANDARDS AND TECH., FRAMEWORK FOR IMPROVING CRITICAL INFRASTRUCTURE CYBERSECURITY (Apr. 16, 2018), https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf.