



BERNARD C. "JACK" YOUNG
MAYOR

*Office of Government Relations
88 State Circle
Annapolis, Maryland 21401*

HB 235

February 12, 2020

TO: Members of the Government Operations and Health Facilities Subcommittee

FROM: Nicholas Blendy, Deputy Director, Mayor's Office of Government Relations

RE: House Bill 235 – State Government – Department of Information Technology – Cybersecurity

POSITION: LETTER OF INFORMATION

Chair Rosenberg and Members of the Subcommittee, please be advised that the Baltimore City Administration submits this **letter of information** on House Bill (HB) 235. HB 235 expands the responsibilities of the Maryland Secretary of Information Technology to include (1) advising and consulting with the Legislative and Judicial branches of State government regarding a cybersecurity strategy and (2) in consultation with the Attorney General, advising and overseeing a consistent cybersecurity strategy for units of State government, including institutions under the control of the governing boards of the public institutions of higher education, counties, municipal corporations, school districts, and all other political subdivisions of the State.

In May of 2019, approximately 7,000 Baltimore City employees could not access their information technology as a result of a ransomware attack that seized operation of these devices. The ransomware attackers demanded approximately \$100,000 in Bitcoin from the City before they would relinquish control. The City went weeks without major services—many of which are public facing, which impacted the ability to access and pay water and sewer bills, access important City information necessary to real property and other industry, as well as numerous internal business functions due to the inability to access critical systems involved in the attack. The City's Office of Finance estimated that this attack cost approximately \$18 million (\$10 million for restoring and repairing

computer networks and \$8 million in potential lost or delayed revenues). As a result of our experience, the City has contracted for a cyberinsurance policy and updated certain policies relating to backups, which should help offset any costs of any future system restoration, should need arise.

HB 235 takes an important step in trying to coordinate a consistent set of cybersecurity policies and procedures to protect units of state and local government around the state from attacks, and highlights the urgency of this issue that the BCA knows well from our experience. Given the current funding levels and present capacity of the Department of Information Technology (DoIT), the BCA imagines that conversations will be evolving around what the appropriate role of resource sharing and responsibilities are between DoIT, the various state agencies that are involved, and the vast number of political subdivisions that would be impacted. The BCA looks forward to participating in these conversation as HB 235 moves forward through the legislative process and other stakeholders add their perspectives.

We thank you for reading our **letter of information** on House Bill 235.