BRIAN E. FROSH
ATTORNEY GENERAL

MEDIA CONTACTS:
PRESS@OAG.STATE.MD.US
410-576-7009

PRESS RELEASE

Attorney General Frosh, Maryland Cybersecurity Council Release Biennial Report

Legislation Protecting Consumers Enacted; Cybersecurity Breach Portal Created

BALTIMORE, MD (July 3, 2017) – Maryland Attorney General Brian E. Frosh, Chair of the Maryland Cybersecurity Council, today announced the release of its Biennial Report, outlining the Council's activities and updated recommendations based on its findings over the last 12 months. The report follows up on its Preliminary Report issued in July 2016, in which several of the Council's recommendations have been implemented. The recommendations include enactment of several bills that expand protections for consumers, the creation of a portal to house best practices and additional resources to protect Maryland's critical infrastructure. "The Council has made progress in its first year, but much remains to be done to protect against threats to Maryland's citizens, critical infrastructure and state operations," said Attorney General Frosh. "The recommendations developed by the Council provide a solid roadmap for addressing cyber security issues."

In Fiscal Year 2016, the Office of Attorney General reported that there were 564 data breaches affecting more than 600,000 Maryland residents. According to the report, these breaches were due to phishing, retail malware, lost or stolen laptops or other devices, unauthorized access, and inadvertent administrative error, such as mistakenly sending personal identifying information to third parties not authorized to have it. In response, in the 2017 legislative session, at the recommendation of the Council, the Maryland General Assembly enacted bills to expand the protections under the Maryland Personal Information Protection Act (SB 525/HB 974) and to waive data breach victims' fees for a credit freeze (SB 270/HB 212), effective January 1, 2018 and October 1, 2017, respectively.

In an effort to assist small and medium-sized enterprises that do not have the deep financial and professional cybersecurity resources of much larger organizations, the Council developed, in partnership with the Maryland Department of Information Technology (DoIT), a one-stop portal housing resources and best practices to help prevent and address cybersecurity infrastructure attacks. The portal will be available in the fall of 2017, and can be found on the Office of Attorney General and the Maryland Cybersecurity Council websites.

The Biennial report also outlined updates on the recommendations the Council provided in its Preliminary Report from July 2016 to advance Maryland's cybersecurity. The recommendations included:

1. Creation of Cyber First Responder Reserve Law, Policy, Legislation
2. Updates to the Maryland Personal Information Protection Act
3. Civil Cause of Action for Remote Unauthorized Intrusions
4. Facilitating Use of the No-charge Credit Freeze Option
5. Inclusion of NIST Cybersecurity Framework in the State IT Master Plan
6. Publication of a Maryland Data Breach Report
7. Integrated Cyber Approach for Mid-Atlantic Region Cyber Operations & Incident Response
8. Educational Resources for Critical Infrastructure Owners and Operators Critical Infrastructure
9. Identify Maryland Critical Infrastructure and Risk Assessments
10. Basic Computer Science and Cybersecurity Education & Workforce
11. Maryland Cybersecurity Scholarship for Service Development
12. Resources for University Computer Science Departments
13. Study of Cyber Workforce Demand and Skills
14. Transition Path for Community College Graduates
15. Increased Funding for Academic Research
16. Cybersecurity Business Accelerators Economic Development
17. Cybersecurity Repository Public Awareness & Outreach

The progress and full summary of each of the recommendations are detailed in the full report.

In 2015, the Maryland General Assembly created, through Senate Bill 542, the Maryland Cybersecurity Council to develop comprehensive strategies and recommendations to protect the State's critical infrastructure. The Council was also tasked with developing strategies to position Maryland as a national hub in cybersecurity innovation and jobs. To achieve its mission and purpose, the Council established six subcommittees, including law, policy and legislation; cyber operations and incident response; critical infrastructure and cybersecurity framework, education and workforce development; economic development; and public awareness and community outreach. The Council's next report is due to the Maryland General Assembly on July 1, 2018.