BRIAN E. FROSH
ATTORNEY GENERAL

MEDIA CONTACTS:
Press@oag.state.md.us
410-576-7009

# PRESS RELEASE

## AG Frosh, Maryland Cybersecurity Council Release Preliminary Report

### *Interim Recommendations Include Creating Cyber First Responders Reserve*

**BALTIMORE, MD (July 1, 2016) -** Attorney General Brian E. Frosh, Chair of the Maryland Cybersecurity Council, and the Maryland Cybersecurity Council, today announced the release of its Initial Activities Report, outlining the Council's activities and preliminary recommendations based on its findings this year. Among those, the Council recommends the State create a cyber first responders reserve, where an appropriate state agency would coordinate with top cyber expert reservists in the event of a cyber emergency.

"Just as you would prepare for a natural disaster, having a plan in the event of a cyber attack is just as imperative for the safety of our citizens," said Attorney General Frosh. "A cyber attack can not only wipe out personal and financial information for thousands of people in mere seconds, it can also take out electric grids and other major infrastructure that are essential to our daily lives. If we had reservists on hand who were trained to combat this specific type of threat, we could minimize the damage, notify the public quicker, and protect valuable information and assets."

Recently the United States government created a digital service corps to facilitate the hiring of digital expertise. In addition, the federal government and individual states have a national reserve that can be called upon in the event of a natural or other kind of disaster. The Council recommends Maryland have access to a reserve of digital expertise, due to the growing threat cyber attacks pose to the welfare of the state. The Council envisions the Maryland Emergency Management Agency leading and coordinating the efforts to build a cyber first responder reserve.

Additional recommendations from the Council include:

- Developing legislation to expand the applicability of the Maryland Personal Information Protection Act (MPIPA) by redefining "personal information" to include more types of data that can be used to identify a person.
- Creating a civil cause of action for remote intrusions, providing a private party the ability to pursue a claim against a person or entity that access the private party's personal information without authority.

- Examining a coordinated approach with other states and government cybersecurity efforts across the Mid-Atlantic region.
- Working with the National Institutes of Standards and Technology (NIST), the U.S. Department of Homeland Security and other government agencies to identify critical infrastructure sectors that are at risk of cyber attacks and are in need of enhanced cybersecurity measures.
- Creating an online repository of cybersecurity outreach, awareness and training information available to individuals, and private and public sectors.

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 move Maryland forward 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 has held three full Council meetings and numerous subcommittee meetings throughout the year.

The interim report was delivered to Maryland General Assembly today. The Council's next report is due to the Maryland General Assembly on July 1, 2017.

The full report and interim recommendations can be found here.