COMMONWEALTH OF PENNSYLVANIA
DEPARTMENT OF BANKING AND SECURITIES

October 27, 2016

To: ALL PENNSYLVANIA STATE-CHARTERED, LICENSED, AND REGISTERED FINANCIAL SERVICES INSTITUTIONS AND COMPANIES:

Financial institutions continue to be a heightened target for cybercriminals and social "hacktivists" and must remain ever vigilant in their efforts to protect their information systems and customers from attack. Companies that do not recognize this threat at the highest levels of the organization chart and that do not take proactive, best-practices cybersecurity approaches to meet this threat will lose the confidence of the marketplace and may lose their customer base, their partners, and their vendors.

The Department continues to work collaboratively with federal regulators, other states financial regulators, and other Commonwealth agencies to address cybersecurity challenges. The Department also will continue to assist its regulated entities by highlighting and providing resources relating to cybersecurity and issues challenging the financial services companies under its supervision.

While not all inclusive the following resources can serve as a starting point for companies to better understand and prepare for cybersecurity challenges in the coming years:

- Presidential Policy Directive (PPD-41) – sets forth principles governing the federal government's response to any cyber incident, and establishing lead federal agencies and an architecture for coordinating for broader federal government response.
- The FFIEC Revised Information Security Booklet – addresses the factors necessary to assess the level of security risks to a financial institution's security program.
- FDIC Cyber Challenge – a series of YouTube videos role-playing in which businesses discuss operational risk issues and the potential impact of information technology disruptions on their business functions.
- SEC's Division of Investment Management guidance – emphasizes best practices and warning compliance officers of the potential securities law violations that could occur due to failure to address deficiencies in cybersecurity programs.

New developments and resources are also discussed in the Cybersection of The Quarter, the Department's quarterly newsletter.

Cybersecurity is a serious challenge of the highest priority, the Department continues to provide resources that can allow companies to discover the best approach to protect themselves, their vendors, their employees, and their customers.

Sincerely, /s/
Robin L. Wiessmann