ICBA
Independent Community Bankers of America®

PRESIDENT'S CYBERSECURITY EXECUTIVE ORDER

CYBERSECURITY

MAY 12, 2017

EXECUTIVE ORDER: "STRENGTHENING THE CYBERSECURITY OF FEDERAL NETWORKS AND CRITICAL INFRASTRUCTURE"

On May 11, 2017, President Trump signed an Executive Order entitled "Strengthening the Cybersecurity of Federal Network and Critical Infrastructure" ("Executive Order").[1] The Executive Order focuses on the modernization of government information technology systems, government capabilities to protect critical infrastructure, promoting an open and secure Internet and promoting development of a cybersecurity workforce.

The first section of the Executive Order focuses on Federal information technology systems. It requires the use of the Framework for Improving Critical Infrastructure Cybersecurity ("Cybersecurity Framework"), developed by the National institute of Standards and Technology, by all Federal departments and agencies to protect the entire executive branch enterprise.

Section two of the Executive Order requires certain reports to be compiled and delivered to the President concerning the authorities and capabilities agencies could employ to support cybersecurity efforts of Section 9 entities, which were identified during the previous Administration.[2] Additionally, the government will engage Section 9 entities and solicit input as appropriate to evaluate whether and how the authorities and capabilities identified by the government may be used to support cybersecurity risk management efforts and any obstacles. Following the initial report, annual reports are required as part of the Executive Order.

Additionally, the Executive Order requires a report to the President regarding the sufficiency of existing Federal policies and practices to promote appropriate market transparency of cybersecurity risk management practices by critical infrastructure entities, with a focus on publicly traded critical infrastructure entities.

Section three of the Executive Order focuses on the promotion of an open and secure Internet. A report is due to the President detailing the Nation's strategic options for deterring adversaries and better protecting the American people from cyber threats. Reports are also required on the development of a cybersecurity workforce in both the public and private sectors.

Finally, the Executive Order also requires reports related to an assessment of a disruption of electricity in the event of a cyberattack and related response capabilities and on cyber risks facing the defense industrial base and supply chain.

[1] https://www.whitehouse.gov/the-press-office/2017/05/11/presidential-executive-order-strengthening-cybersecurity-federal

[2] See Executive Order 13696, Section 9. On February 19, 2013, President Obama signed an Executive Order entitled "Improving Critical Infrastructure Cybersecurity". In the Executive Order, Section 9, the President ordered an identification of critical infrastructure firms in which a cybersecurity incident could reasonably result in catastrophic regional or national effects on public health or safety, economic security or national security. The list of identified firms is confidential. In the financial service sector, these are generally very large financial institutions.