WILLKIE FARR & GALLAGHER LLP

NEW YORK WASHINGTON HOUSTON PARIS LONDON FRANKFURT BRUSSELS MILAN ROME

CLIENT MEMORANDUM

Presidential Commission on Enhancing National Cybersecurity Has Issued Recommendations and Action Items for Securing the Digital Economy

December 5, 2016

AUTHORS

Daniel K. Alvarez | Elizabeth J. Bower | James R. Burns | James C. Dugan | Elizabeth P. Gray | Katherine Doty Hanniford | Naomi E. Parnes

On December 2, 2016, the Commission on Enhancing National Cybersecurity released its Report on Securing and Growing the Digital Economy ("Report"). President Obama created the bipartisan Commission by Executive Order in February 2016 and tasked it with assessing the state of the nation's cybersecurity and developing actionable recommendations for securing and growing the digital economy. The Commission's recommendations aim to achieve enhanced cybersecurity while also protecting privacy and civil liberties, ensuring public safety and economic and national security, and fostering innovation.

The Report identifies six imperatives for enhancing cybersecurity, and sets forth 16 recommendations and 53 associated action items supporting the imperatives. The six imperatives are:

1. Protect, defend, and secure today's information infrastructure and digital networks.
2. Innovate and accelerate investment for the security and growth of digital networks and the digital economy.
3. Prepare consumers to thrive in a digital age.

4. Build cybersecurity workforce capabilities.

5. Better equip government to function effectively and securely in the digital age.

6. Ensure an open, fair, competitive, and secure global digital economy.

Several of the recommendations and action items are directed toward the first 100 days of the Trump Administration, but it is unclear which items will be addressed and implemented. The President-elect has stated that cybersecurity is a top priority of his administration, however, so there is reason to believe that the recommendations in the Report will continue to be relevant. Moreover, some aspects of the Report may be relevant regardless of how the new Administration treats the recommendations; for example, the Report recommends the establishment of best practices for Internet of Things ("IoT") cybersecurity and privacy that may be used as a benchmark against which parties' practices are measured. The Report highlights that the line between critical infrastructure and everything else is blurring rapidly as technology becomes more interdependent.

The Report highlights three roles for government in this space which will have an effect on private sector enterprises: (1) government as partner, developing greater public-private collaboration; (2) government as regulator, to ensure that companies provide enhanced information to consumers and take steps to secure their products and services; and (3) government as facilitator, to incentivize cybersecurity and foster innovation. The related recommendations are detailed below.

Government as Partner: Greater Public-Private Partnership to Achieve Security

The Report focuses on the importance of collaboration between the public and private sectors, and includes a number of recommendations consistent with that focus. For example:

- The private sector and the Administration should launch a joint cybersecurity operations program to collaborate on cybersecurity activities in order to identify, protect from, detect, respond to, and recover from cyber incidents affecting critical infrastructure.

- The federal government provides companies with the opportunity to engage proactively and candidly in formal collaboration with the government to advance cyber risk management practices and to establish a well-coordinated joint defense plan based on the principles of the National Institute of Standards and Technology ("NIST") Cybersecurity Framework ("NCF"). In particular, the Report encourages the Department of Homeland Security ("DHS") to work with industry to implement protections under the statutory Protected Critical Infrastructure Information Protections that would encourage companies to more freely share information about their practices while protecting their documents, communications, and deliberations from public disclosure under transparency laws; discovery in litigation; use in regulatory enforcement investigations or rule-makings; and waiver of client privilege.

- Federal agencies expand the current implementation of the information-sharing strategy to include exchange of information on organizational interdependencies within the cyber supply chain. For example, the Report recommends broadening the cyber threat indicator sharing under the Cybersecurity and Information Sharing Act that currently takes place at the DHS National Cybersecurity and Communications Integration Center ("NCCIC"), which houses the Automated Indicator Sharing ("AIS") capability.

- The federal government and private sector join forces to improve IoT security.

The Report also helps clarify the roles and responsibilities of the private and public sector in the wake of cybersecurity events, for example by stating that the federal government bears ultimate responsibility for the nation's defense and security.

Government as Regulator: Enhanced Information for Consumers and Potentially New Regulations?

The Report includes a number of recommendations that could impose additional burdens on private enterprise, either through enhanced disclosures to consumers or a greater role for regulators. For example, the Report recommends that:

- Business leaders in the information technology and communications sectors should work with consumer organizations and the Federal Trade Commission ("FTC") to provide consumers with better information so that they can make informed decisions when purchasing and using connected products and services.

- An independent organization should develop a cybersecurity "nutrition label" for technology products and services that consumers will intuitively trust and understand.

- The FTC, in conjunction with consumer organizations and industry, should develop a standard template for documents that inform consumers of their cybersecurity roles and responsibilities and a "Consumer's Bill of Rights and Responsibilities for the Digital Age." In addition to educating consumers of their rights and clarifying privacy protections, the "cybersecurity bill of rights" would articulate the responsibilities of all citizens that participate in the digital economy.

- Federal agencies harmonize existing and future regulations with the NIST Cybersecurity Framework to focus on risk management, in order to reduce the private sector's cost of complying with prescriptive or conflicting regulations that may not aid cybersecurity and may unintentionally discourage rather than incentivize innovation.

In light of the President-elect's stated de-regulatory approach, these recommendations seem least likely to be implemented. However, these recommendations likely will form the foundation of any future debate regarding regulation in this space.

Government as Facilitator: Incentivizing Cybersecurity and Fostering Innovation

One of the primary themes of the Report is the importance of ensuring that security does not stifle innovation. The Commission advises that incentives are to be preferred over regulation. The Commission further recommends that the federal government extend additional incentives to companies that have implemented cyber risk management principles and demonstrate collaborative engagement.

While the extent to which the Trump Administration will embrace the Report's recommendations and action items remains unknown, the Report provides an expansive articulation of the current state of play of cybersecurity readiness as it relates to the intersection of cyber security and the digital economy. The Report is noteworthy for its identification of a set of priorities for private sector participants within the digital economy. Bearing in mind the recent cyber attacks related to the IoT and Distributed Denials of Service ("DDoS"), the Report's identification of such cybersecurity threats and the call for improvements may actually serve to heighten corporate obligations to defend against subsequent IoT and DDoS threats, notwithstanding any action (or inaction) on the part of the new Administration and the Report's recognition of the extent and severity of the threat as one that merits regulatory attention.

Pursuant to the Executive Order by which it was created, the Commission shall be terminated by December 17, 2016 unless extended by President Obama.

If you have any questions regarding this memorandum, please contact Daniel K. Alvarez (202-303-1125, dalvarez@willkie.com), Elizabeth J. Bower (202-303-1252, ebower@willkie.com), James R. Burns (202-303-1241, jburns@willkie.com), James C. Dugan (212-728-8654, jdugan@willkie.com), Elizabeth P. Gray (202-303-1207, egray@willkie.com), Katherine Doty Hanniford (202-303-1157, khanniford@willkie.com), Naomi E. Parnes (202-303-1225, nparnes@willkie.com) or the Willkie attorney with whom you regularly work.

Willkie Farr & Gallagher LLP is an international law firm with offices in New York, Washington, Houston, Paris, London, Frankfurt, Brussels, Milan and Rome. The firm is headquartered at 787 Seventh Avenue, New York, NY 10019-6099. Our telephone number is (212) 728-8000 and our fax number is (212) 728-8111. Our website is located at www.willkie.com.

December 5, 2016