O'Melveny

Alerts & Publications

President Obama's Cybersecurity Commission Releases Findings and Recommendations

December 5, 2016

KEY CONTACTS

Matthew W. Close
Los Angeles
D: +1-213-430-7213

Thomas E. Donilon
Washington, DC
D: +1-202-383-5333

Randall W. Edwards
San Francisco
D: +1-415-984-8716

On Friday, December 2, 2016, President Obama's Commission on Enhancing National Cybersecurity released a report detailing its findings and recommendations on improving cybersecurity in the public and private sectors. The Commission, which was led by O'Melveny Vice-Chair Tom Donilon, was charged with making short- and long-term recommendations to strengthen the security of our digital economy.

The Commission identified and considered broader trends, most notably: the convergence of information technologies and physical systems, the need to reorganize US government structures and practices to address cyber threats, the importance of a risk-management (as opposed to a purely compliance-based) approach to cybersecurity, the growing interdependence of nations in the global cyber sphere, the effectiveness of free markets versus regulatory and liability solutions, the need to develop meaningful cybersecurity metrics, and the rights and responsibilities of the consumer. In these areas and others, the Commissioners examined what is working well, where challenges persist, and what needs to be done to incentivize and cultivate a culture of cybersecurity in the public and private sectors.

The report identifies six imperatives for enhancing cybersecurity, along with specific recommendations and action items. For each imperative, the Commission calls for increased collaboration between the government and private sector. Highlights include recommendations to:

- Form a joint body, the National Cybersecurity Private-Public Program, modeled after the President's Intelligence Advisory Board, to advise the President on cyber issues and encourage public-private collaboration.
- Extend the NIST Framework by using it as the basis for harmonizing disparate regulations, requiring its use among all government agencies, developing metrics and guidance to promote its use in the private sector, and utilizing it as the basis for international standard-setting.
- With respect to identity management, form a national public-private initiative to encourage "strong authentication" that will move us beyond the password.
- Develop minimum security standards for connected devices (commonly known as "IoT") through a joint public-private process.
- Invest in R&D that focuses on moving security away from the end user.

- Launch a national public-private consumer awareness campaign within the first 100 days of the next Administration. Part of that initiative would include the development of a standardized "cyber nutrition label" to go on digital products, in order to inform the consumer of a product's cybersecurity risks and features.
- Encourage the FTC to take the lead in developing a "Consumer Bill of Rights" that would inform citizens of their rights and responsibilities in the digital age.
- Develop a "workforce surge" that would increase the number of cybersecurity practitioners in the US by 150,000 by the year 2020 by (1) building a national cybersecurity program modeled on the White House's TechHire program to train and hire cybersecurity practitioners and (2) creating a national apprentice program that creates pathways for students from two- and four-year colleges.
- Continue to promote peacetime cybersecurity norms of behavior, particularly through the use of Mutual Legal Assistance Treaties (MLATs).

The report has been commended by cybersecurity experts as a "quality set of recommendations," with specific praise for the report's focus on the emerging risk posed by the Internet of Things and its plans for a consumer cybersecurity awareness and engagement campaign. For additional coverage on the report, please see "Presidential Commission Sounds Warning Over Botnet Threat," *Wall Street Journal*, and "White House Should Lead Broad Cybersecurity Effort: Panel," *AFP*.

If you have any questions on the report, please contact O'Melveny's Data Security and Privacy Group, which helps clients manage the serious legal and financial risks in this rapidly changing area, taking an approach that crosses borders and legal disciplines. The Group includes Donilon, President Obama's former National Security Advisor; a former Cabinet Secretary and Senior Advisor to the President; a former Senior Counsel to the President; a former Deputy Secretary of Commerce; a former Director of the Federal Trade Commission's Bureau of Competition; and a former resident legal advisor to the US Embassy in Beijing and federal cybercrime prosecutor.

---

licensed to practice law in California, Thomas Donilon, an O'Melveny partner licensed to practice law in the District of Columbia, Danielle Gray, an O'Melveny partner licensed to practice law in New York, Randall Edwards, an O'Melveny partner licensed to practice law in California, and Jeremy Maltby, an O'Melveny partner licensed to practice law in California, the District of Columbia and New York contributed to the content of this newsletter. The views expressed in this newsletter are the views of the authors except as otherwise noted.