Akin Gump
STRAUSS HAUER & FELD LLP

Cybersecurity, Privacy & Data Protection Alert

December 15, 2016

Key Points

- The distinguished Commission on Enhancing National Cybersecurity, established by President Obama and tasked with assessing the state of our cybersecurity and developing actionable recommendations that could assist the next administration, issued its 90-page *Report on Securing and Growing the Digital Economy* on December 1.
- The report provides a range of analysis and recommendations, as well as 53 action items that include ambitious ideas designed to provide a way forward and to improve cybersecurity for businesses, government and consumers that it states can begin to be implemented in the short and medium term.
- The report includes recommendations and action items to address liability concerns and incentives for businesses to appropriately manage cybersecurity risks; ways to reorganize how the federal government protects its own digital information; and novel ways to inform consumers about the cybersecurity health of various products and services.

Obama Commission on Enhancing National Cybersecurity Provides Recommendations to Next Administration

In April 2016, President Obama appointed the Commission on Enhancing National Cybersecurity (the "Commission") to assess the state of our cybersecurity and develop actionable recommendations for securing the digital economy as it advances, in part to assist the next administration. Led by his former National Security Advisor Tom Donilon and comprised of experts from outside government aided by staff from several federal agencies to help gather and analyze information, the Commission issued its 90-page *Report on Securing and Growing the Digital Economy* on December 1 (the "Report"), presenting numerous recommendations and action items, some of them interesting and provocative.[1]

A significant portion of the analysis and some of the recommendations should be of interest to the incoming Trump team as it moves forward with its own plans to have a Cyber Review Team that includes

[1] Commission on Enhancing National Cybersecurity: Report on Securing and Growing the Digital Economy (Dec. 1, 2016), https://www.whitehouse.gov/sites/default/files/docs/cybersecurity_report.pdf. The page count includes the appendices.

government and private sector representation and will be led by the Department of Defense (DoD), to conduct a far-ranging cybersecurity review of U.S. cyber defenses and vulnerabilities, including critical infrastructure and other important areas; and to create joint task forces throughout the U.S. to coordinate federal, state, and local law enforcement efforts against cybercrime.

The Report by the Numbers

- The Commission's 12 members included individuals recommended by leaders of both parties in the House and Senate and others selected by the President. These included, in addition to Chairman Tom Donilon, the former National Security Advisor to President Obama, the Commission's Vice Chair, Samuel Palmisano, the former Chairman and CEO of IBM, and a host of distinguished leaders and experts from academia and industry, including several CEOs, some of whom had previously held critical government roles.
- In developing the Report, the Commission obtained a wide range of input, including testimony from six hearings it held across the country and from numerous written comments received in response to its public solicitations.
- The Report identifies 10 foundational principles, nine broad findings, six major imperatives, 16 recommendations and a total of 53 action items associated with those recommendations.
- Each action item includes guidance regarding when the Commission believes work on it should commence. All were designated for the short or medium term, ranging from the first 100 days to five years, depending on whether action is required by both Congress and the Administration, or extensive consultation with other stakeholders is required, or if more information is needed.
- The nine broad findings state that many organizations still fail to do even basic cybersecurity. Companies are under pressure to move innovations to market quickly, even at the expense of cybersecurity; flexible and mobile working environments are necessary but increase risk and make the "classic concept of the security perimeter…largely obsolete"; technological complexity creates vulnerabilities and sophisticated attackers can gain access at a fraction of the cost of defense; risks from increased connectivity are sometimes associated with the Internet of Things ("IoT"); interdependencies, decentralization and supply chain risks abound; government is vexed by large legacy technology systems and challenges in making investments in and procuring needed talent and systems; and concern is increasing and trust eroding in everything from the integrity of data, elections, and organizations that produce products and services.

Action Items

The array of action items suggested by the Commission include ideas that are designed to provide a way forward to improve cybersecurity for businesses, government and consumers. Some of the action items will be appealing to the business community, others may be neutral, and still others may be regarded with skepticism or concern.

Here are some examples of the action items:

- The Department of Homeland Security (DHS) should work to address industry's concern about increased exposure to legal actions if it engages with government proactively and collaboratively on a coordinated joint defense plan and risk management practices, by working with industry to identify needed changes in statutes, regulations or policies such as public disclosure laws like FOIA, discovery in civil litigation, use in regulatory enforcement actions or rulemaking, implications for attorney-client privilege, or similar concerns. Action Item 1.2.3
- The National Institute of Standards and Technology (NIST) should build on its Cybersecurity Framework and establish a Cybersecurity Framework Metrics Working Group (CFMWG) to develop industry-led, consensus-based metrics that industry can use to voluntarily assess relative corporate risk, help government and insurers to understand insurance coverage needs and standardize premiums, and implement a nationwide voluntary incident reporting program for identifying cyber gaps. Action Item 1.4.1
- Federal regulators should harmonize existing and future regulation with the NIST Cybersecurity Framework to address strong private sector concerns that regulators are inconsistently using and applying the Framework; and are creating redundancy, inconsistency, higher compliance costs for businesses, and impediments to innovation. In addition, the Report calls for the creation of Office of Management and Budget (OMB) procedures to reduce the likelihood of these federal problems and also calls for state and local regulatory agencies to address overlapping and potentially inconsistent state regulation. Action Item 1.4.3
- The government should create additional incentives to companies that implement cyber risk management principles and demonstrate collaborative engagement, such as liability protections, including certain safe harbors for companies in regulated sectors. Additional incentives might include tax and government procurement incentives, prioritized cyber technical assistance, regulatory streamlining or public recognition. Action Item 1.4.5
- The Department of Justice (DOJ) should lead an interagency study with governmental and private parties to assess whether the law provides appropriate incentives for companies to design security into their products, including in regard to liability for harm caused by faulty IoT devices. This includes whether there are adequate protections for companies that do adequately design-in cybersecurity and identification and action regarding any gaps. Action Item 2.1.3
- Independent organizations should develop the equivalent of a cybersecurity "nutritional label" for technology products and services to provide consumers better information to make informed choices, perhaps linked to understandable and impartial third-party ratings. Action Item 3.1.1
- The General Services Administration (GSA) should lead efforts to integrate technology across government more effectively and share standard platforms, and improve federal procurement by involving agency CISOs, creating integrated teams of agency technology and acquisition experts, and reforming the procurement and bid protest process. Action Item 5.2.2

- To address a lack of standards of measurement in assessing cybersecurity preparedness, the CFMWG should develop metrics to assess an agency's cybersecurity posture and integrate the metrics with other relevant measures to evaluate performance as part of the annual budget process. Action Item 5.3.3
- Congress should consolidate cybersecurity and infrastructure protection functions under the oversight of a single federal agency with appropriate capabilities and responsibilities to do the job. Action Item 5.5.2
- The President should appoint an Ambassador for Cybersecurity as part of a federal government effort to build consensus, standards and norms to harmonize U.S. and international approaches to cybersecurity and avoid inconsistencies that create unnecessary costs. See, e.g., Action Items 6.1.1, 2, 3.

In a written statement,[2] President Obama urged President-elect Trump and the next Congress to consider the recommendations. The President said, "The Commission's recommendations are thoughtful and pragmatic…I believe that the next administration and the next Congress can benefit from the Commission's insights and should use the Commission's recommendations as a guide." President Obama also asked the Commission to brief President-elect Trump and his transition team on the report "at their earliest opportunity."[3]

[2] Statement by the President on the Report of the Commission on Enhancing Cybersecurity (Dec. 2, 2016), https://www.whitehouse.gov/the-press-office/2016/12/02/statement-president-report-commission-enhancing-national-cybersecurity.

[3] *See* the penultimate paragraph of the Statement by the President on the Report of the Commission on Enhancing Cybersecurity (Dec. 2, 2016), https://www.whitehouse.gov/the-press-office/2016/12/02/statement-president-report-commission-enhancing-national-cybersecurity.

Contact Information

If you have any questions regarding this alert, please contact the Akin Gump lawyer with whom you usually work or:

Natasha G. Kohne
nkohne@akingump.com
+971 2.406.8520 | Abu Dhabi
+1 415.765.9500 | San Francisco

Michelle A. Reed
mreed@akingump.com
+1 214.969.2713 | Dallas

David S. Turetsky
dturetsky@akingump.com
+1 202.887.4074 | Washington, D.C.

Greg W. Guice
gguice@akingump.com
+1 202.887.4565 | Washington, D.C.

Crystal Roberts
cgroberts@akingump.com
+1 415.765.9560 | San Francisco