AN EPUBLICATION OF THE LOS ANGELES COUNTY BAR ASSOCIATION

LACBA

PRIVACY AND CYBERSECURITY SECTION

Section Home Page
click here ›

JUNE 2020

Back to June 2020 issue

Rethinking Cybersecurity - the Cyberspace Solarium Commission's Plan

EILEEN M. DECKER, Pacific Intelligence & Cyber and former U.S. Attorney

On March 11, 2020, the day the World Health Organization declared COVID-19 a pandemic, the Cyberspace Solarium Commission ("Commission") issued its highly anticipated report.[1] Although the report was well received, the release of the Commission's report received only modest attention due to the ongoing public health emergency.[2] This may change, however, since Congressional hearings on the report and its recommendations began on Wednesday, May 13th. The Commission's report will also be the subject of a June 11, 2020 webinar hosted by the Los Angeles County Bar Association's Privacy & Cybersecurity Section, which will feature members of the Commission who will discuss different aspects of the report and its conclusions, and members of the Los Angeles legal community who will discuss the report's local impact.

The Commission was modeled after President Eisenhower's 1953 Project Solarium, designed to address the then-growing threat posed by the Cold War. The persistent and increasing threat created by the absence of robust cybersecurity was, instead, this Commission's mission. Established under the fiscal year 2019 John S. McCain National Defense Authorization Act, the Commission was charged with creating bipartisan recommendations to redesign the nation's cybersecurity strategy. The challenge in effectively addressing cybersecurity was succinctly observed in the report:

> The digital connectivity that has brought economic growth, technological dominance, and an improved quality of life to nearly every American has also created a strategic dilemma. The more digital connections people make and data they exchange, the more opportunities adversaries have to destroy private lives, disrupt critical infrastructure, and damage our economic and democratic institutions.[3]

[1] Cyberspace Solarium Commission Report ("Report"), March 2020. The Report can be accessed at: https://www.solarium.gov/report

[2] Media Reports on the Commission, the Report and its recommendations can be found at: https://www.solarium.gov/press-and-news.

[3] Report, at 1.

The 174-page report contains over 75 recommendations aimed at reforming the nation's approach to cybersecurity. The recommendations are categorized under six pillars, specifically: (1) Reform the U.S government's structure and organization; (2) Strengthen norms and non-military tools; (3) Promote national resilience; (4) Reshape the cyber ecosystem toward greater security; (5) Operationalize cybersecurity collaboration with the private sector; and (6) Preserve and employ the military instrument of power.[4]

The combined recommendations seek to alter the risk calculation made by the nation's adversaries, and make it more costly and less profitable for them to engage in malicious cyber activity aimed at U.S entities. To do so, the Commission argues that the U.S. must work with its allies and partners to promote responsible behavior in cyberspace, deny benefits to adversaries who exploit vulnerabilities in cyberspace, and impose costs by retaliating against adversaries who target the nation.[5] The report seeks to bring strategic coherence to the nation's cybersecurity approach and recommends restructuring the U.S. government by elevating the Department of Homeland Security's Cybersecurity and Infrastructure Security Agency ("CISA") to a more prominent role within the government to enable it to promote a more secure cyber ecosystem,[6] and establishing a National Cyber Director within the Executive Office of the President.[7]

In addition, the Commission recommends that the U.S. collaborate more closely with the private sector, recognizing that: "The majority of assets, functions, and entities in the cyber domain that are attractive targets for adversaries are owned and operated by the private sector."[8] As a result, the Commission seeks to build a framework for improving and prioritizing U.S. government cybersecurity support to critical elements of the private sector, improve information sharing in order to create better situational awareness of cyber threats within the private sector, and better integrate cyber defense security efforts within the private sector.[9]

Specific recommendations that impact the private sector also include establishing final goods assembler liability for incidents that exploit known and unpatched vulnerabilities;[10] passing a National Breach Notification Law which would preempt the existing state data breach laws and create a single standardized federal notification system;[11] creating a National Cybersecurity Certification and Labeling Authority to establish a standardized language for a labeling system to provide consumers with information on the security characteristics of software and hardware;[12] and amending the Sarbanes-Oxley Act to require the disclosure of issues associated with cybersecurity risks.[13]

In order to create policies to better deal with cyberattacks, policymakers and analysts need greater insights into the severity and scope of these attacks. To that end, the Commission recommends Congress create a Bureau of Cyber Statistics (modeled after the Bureau of Labor Statistics) within the Department of Commerce

[4] Id. at 1-7, 123-26.
[5] Id. at 1.
[6] Id. at 39.
[7] Id. at 37.
[8] Id. at 96.
[9] Id. at 97-104.
[10] Id. at 76.
[11] Id. at 94.
[12] Id. at 72-74.
[13] Id. at 83.

to collect and provide statistical data on cybersecurity and the cyber ecosystem. The specific types of cyber data to be collected are not identified, but the stated objective of the collection process is to define the national cyber risk, help the insurance industry to create more accurate risk models, and help the government craft more effective cybersecurity policies and programs.[14]

To emphasize the urgency to adopting its recommendations, the Commission observes that the "The United States thus stands at a strategic inflection point"[15] in moving forward on reorienting itself to face the cyber challenge. The adversarial landscape is challenging and growing more complex with advancing technology:

> While America looks forward to the potential of cyberspace and associated technologies to improve the quality of human life, threats continue to grow at an accelerating pace. America is facing adversary nation-states, extremists, and criminals that are leveraging emerging technologies to an unprecedented degree. Authoritarian states seek to control every aspect of life in their societies and export this style of government…. Technological trends are creating markets and practices that challenge the U.S. government's ability to provide the stability required for freedom and prosperity to flourish.[16]

To address these escalating challenges, the report emphasizes the critically important role the private sector plays in promoting national cybersecurity. This is particularly true since "the private sector is the hub for technological innovation, with the government at times struggling to import that innovation back into its own systems and processes." [17] The report recognizes that the private-sector's ownership of most of the physical and logical layers of cyberspace results is an "unprecedented reversal of dependencies: while the U.S. government has traditionally provided for the collective defense, it now requires enhanced cooperation and partnership with the private sector."[18]

These interdependencies and the partnerships required to achieve national cybersecurity objectives are now the focus of the Commission's efforts to implement their recommendations, and reorient the nation to adjust to the realities of the cyber threat and the collective effort necessary to address this persistent problem. Many of their recommendations are expected to be included in the fiscal year 2021 National Defense Authorization Act. Reportedly the Commission is not stopping with the release of the report but is now contemplating adding new recommendations based on the cybersecurity issues that became evident across the nation following the onset of the COVID-19 virus.

[14] Id. at 78.
[15] Id. at 19.
[16] Id.
[17] Id.
[18] Id.

Back to June 2020 issue