wiley

NEWSLETTER

The Past is Prologue: A Cyber Preview for 2021

December 2020

Privacy in Focus®

As we all look forward to closing the book on 2020 and await the promise of a new year, we can see the coming landscape in cybersecurity and cyber policy will be heavily influenced by developments and events from this past year. Chief among these influences will be the coronavirus (COVID-19) pandemic. Based upon its size and complexity, the nation's response to COVID-19 has focused policy discussions on broader resilience measures, and both cyber issues and cybersecurity are foundational to these concepts. The pandemic's major disruptions to health care, business operations, education, supply chain management, remote work, e-commerce, and the provision of critical public services are just a few areas where these real-world impacts also have discrete and distinct cyber aspects. And as we have seen, connectivity has been essential to each, meaning reliability in communications technology is top of mind.

While reverberations from COVID-19 will cascade through the policy process for years, we expect trends to manifest in 2021. These themes will fall into three categories: 1) the push for more government oversight of the private sector's cyber posture, 2) the expansion of cybersecurity into a wider array of security and resilience measures, and 3) the need to define the scope of public-private partnerships in cyberspace.

The Cyberspace Solarium Commission and Federal Cyber Initiatives Provide a Roadmap

Authors

Megan L. Brown
Partner
202.719.7579
mbrown@wiley.law

Practice Areas

Privacy, Cyber & Data Governance
White Collar Defense & Government Investigations

In March 2020 and over the following months, the Cyberspace Solarium Commission (CSC) published a report and three white papers containing recommendations to Congress, the Executive branch, and the private sector to better position the nation to respond to cyber threats. Of 99 recommendations in the Solarium Commission Report and three white papers, *Cybersecurity Lessons from the Pandemic* (Pandemic), *Growing a Stronger Cyber Workforce* (Workforce), and *Building a Trusted ICT Supply Chain* (Supply Chain), 56 are intended to be taken up in legislation, and many others rely on administrative actions from agencies such as the Department of Homeland Security (DHS), the National Institute of Standards and Technology (NIST), the Department of Defense (DOD), the Department of Commerce, and the Federal Communications Commission (FCC). Importantly, while these recommendations are targeted at actions in the public policy and legislative space, they could have widescale impacts on the private sector to include companies doing business with the federal government and industry members supporting the nation's critical infrastructure. While a handful of the Commission's proposals have been included in the 2021 National Defense Authorization Act (NDAA), there are still a number of recommendations that have drawn the interest of legislators and policymakers. This, combined with a proposed two-year extension of the Commission's sunset period, potentially positions the CSC's work as driving much of the cyber agenda in the coming year.

On the federal initiatives front, 2020 was a pivotal year and many agencies began to lay considerable groundwork for cyber activities that will carry into the next year and beyond. For example, this past year the Department of Defense took steps and put out rulemaking to develop a cybersecurity certification regime for contractors and suppliers. Similarly, DHS and the Cybersecurity and Infrastructure Security Agency (CISA) began to take a more assertive role with regard to civilian agency cyber practices, utilizing binding operational directives to enforce compliance. Last, the National Institute of Standards and Technology spent considerable time in 2020 assessing and developing guidance on a wide-range of cyber issues to include security for internet-connected devices, or the "Internet of Things" (IoT), and artificial intelligence applications. While this represents only a sampling of federal activity in this space, many of these activities will shape the debate in the years to come. More broadly, these cyber activities in the federal space will also have far-reaching impacts internationally, which is an additional area the U.S. private sector will need to follow. Disparate issues – ranging from infrastructure cyber resilience, to nation state intellectual property theft, to the utilization of active or offensive cyber measures as part of a defense strategy – all will have impacts on U.S. companies, and how the federal government approaches the international community will be important to follow.

Cyber Measures and Increasing Directive Control

The Executive branch has been undertaking several initiatives and utilizing existing authorities to set baseline cybersecurity standards for critical infrastructure sectors and companies looking to do business with the federal government. In the coming year, private-sector organizations can expect to see the federal government take a more directive role in setting security standards through more stringent procurement authorities or new legislative provisions that grant agencies the authority to set cyber standards.

- **Procurement as Enforcement:** Setting the stage in 2020, the Department of Defense, in collaboration with the Office of Management and Budget (OMB), released a long-awaited interim rule to implement

not one, but two new frameworks for verifying contractor compliance with cybersecurity requirements: (1) NIST SP 800-171 DOD Assessment Methodology and (2) the Cybersecurity Maturity Model Certification (CMMC). Over the next five years, DOD will be implementing these new requirements and plans to have all contracts, with some exceptions, covered by this new framework with the requirements falling to both prime and subcontractors. While these provisions and requirements will initially impact defense-related industries, civilian federal agencies will be watching closely and assessing how these certification models map onto non-defense-related contracts.

- **Directive Legislative Authorities:** On November 17, 2020, by unanimous consent, the United States Senate passed bipartisan legislation to secure internet-connected devices – *The Internet of Things (IoT) Cybersecurity Improvement Act of 2020*. Building on ongoing IoT security efforts underway at NIST, the Act sets various workstreams into motion, including to both study IoT security and to develop baseline security requirements for devices purchased through the federal acquisition process. Interestingly, passage of this provision was one of the Solarium Commission's recommendations in the March 2020 report. Policymakers may look to other CSC recommendations such as setting standards for the security of foundational internet protocols and email, or liability on final goods assemblers for additional directive legislative measures.

Expansion of Cyber Issues Beyond Networks and Devices

The COVID-19 pandemic has exposed vulnerabilities across critical infrastructure sectors and the ability to provision critical public services in an environment that increasingly relies on a remote workforce and networked devices. In the coming year, after-action examinations of the nation's response to COVID-19 will be broad and cross-cutting, pulling in both government action and critical services provided to the public by the private sector, and cyber issues will be at the forefront of these conversations.

- **Supply Chain Is Critical to Cyber Resiliency:** In the CSC white paper on the *Supply Chain,* the Commission identifies what it sees as three principle risk vectors that the U.S. needs to address in the information and communications technology (ICT) supply chain ecosystem: readily available raw materials, stock, and inventory of intermediate goods and finished products; the trustworthiness of foreign-sourced equipment and components; and overreliance on foreign manufacturers for ICT technologies. This analysis tracks with other reports and evaluations completed at the end of 2020, to include a report completed by the ICT Supply Chain Risk Management Task Force's (SCRM), COVID-19 Impact Study Working Group (Study Group) and another completed by the Homeland Security Advisory Committee on ICT Risk Reduction. Taken together, these evaluations will set the stage for supply chain specific policy developments in the coming year, many of which may include directive recommendations from the CSC like the need to develop an industrial base strategy for ICT providers.
- **National Critical Functions (NCF) and Cyber Resilience:** In April 2019, the Cybersecurity and Infrastructure Security Agency (CISA) published a list of over 50 national critical functions, which are "functions of the government and private sector so vital to the United States that their disruption, corruption, or dysfunction would have debilitating effect on [the] security, national economic security, [or] national public health or safety" of the country. Importantly, the NCF framework has been adopted

as a foundational principle in several national-level cyber strategies, to include the National Cyber Strategy, the DHS Cybersecurity Strategy and the National Strategy to Secure 5G. During the pandemic, these national critical functions played an increasingly pivotal role in the nation's response to the crisis, helping to both organize response priorities and ensure the provision of critical services and communications to the public. The cross-cutting nature of the NCFs tracks with recommendations from the ICT SCRM COVID-19 report and the CSC white paper on the pandemic. Taken together, policymakers and legislators will likely look to the NCF framework in the coming year to both prioritize critical sectors for heightened cyber standards or move to further regulate industries supporting certain NCFs.

Emphasis on Public-Private Partnerships

As reflected above, this year has demonstrated how the public and private sectors are inextricably linked in the nation's effort to secure the cyber ecosystem. This symbiotic relationship has been the cornerstone of federal cyber strategy and will continue to be a central feature in the coming year. While there are areas where private sector and government interests align, there also are areas of tension that will frame some of the policy debate in 2021.

- **Reporting Requirements and Information Sharing:** In the CSC report and subsequent white papers, there are a number of recommendations aimed at increasing information sharing between the government and private sector, both from the government sharing persistent or nation-state threat information and also from the private sector in sharing critical vulnerabilities or reporting cyber incidents or breaches. The Commission even goes so far as to recommend mandatory vulnerability or incident reporting requirements on the private sector, by amending the Sarbanes-Oxley Act or placing unique requirements on critical infrastructure providers. Outside of the Commission's work, the government has additionally undertaken initiatives such as mandatory vulnerability disclosure programs to increase the government's visibility into networks and systems supporting federal operations. The distinction between proscriptive information sharing and voluntary arrangements will be a central debate in the coming year, especially through federal or defense-related appropriations vehicles.
- **Ransomware:** At the end of October, CISA, in coordination with the Federal Bureau of Investigation (FBI) and the Department of Health and Human Services (HHS), issued a joint advisory about a series of criminal attacks on U.S. hospitals and health care providers using derivations of common ransomware campaigns. This follows a September release from CISA and the Multi-State Information Sharing & Analysis Center (MS-ISAC), who jointly published a comprehensive Ransomware Guide to assist organizations with both mitigation measures and recovery best practices to respond to a ransomware incident. While long a concern of the law enforcement community, the recent advisories about the prevalence of ransomware attacks on organizations and sectors critical to the COVID-19 response highlight how even basic cybersecurity and cyber hygiene practices can prevent virtual disruptions from having an outsized impact in the physical world. Given the context and circumstances that will surround the cyber policy debate in the coming year, the prevalence and spread of ransomware should undoubtably be a central factor in those discussions.

Concluding Thoughts

Cybersecurity policy has a tendency to react to incidents or events impacting the efficient function of the private sector and government operations, and thus, it remains difficult to accurately predict what and which issues will take precedence in the coming year. Changes in the Administration and in Congress will impact these debates, but it is important to recognize that many of these issues have been percolating in the federal cyber community. While matters of execution may differ after a change in Administration, broad strategic objectives have crossed party lines.

The private sector should be looking for ways to engage government, document and explain its approach to cyber risk management, and get a handle on the myriad issues that may cause government to take a more assertive approach. To preserve and maintain key public-private partnerships, companies may increasingly need to earn the trust of an increasingly wary government.