wiley

NEWSLETTER

Highly Anticipated Cyberspace Solarium Commission Report Recommends Major Overhaul in the Nation's Approach to Cybersecurity

March 2020

Privacy in Focus®

On March 11, 2020, the Cyberspace Solarium Commission (CSC or Commission) released its highly anticipated report (Report), containing a host of legal and policy recommendations and signaling a fundamental shift—and "strategic adjustment"—to address cybersecurity risks facing the United States. The Report, which is based upon the strategic principle of "layered cyber deterrence" and proposes a "Whole-of-Nation" approach to addressing evolving and consequential cyber threats, contains dozens of key recommendations spread across six core pillars. If adopted, these recommendations would result in substantial changes for the federal government, as well as significant changes in expectations and obligations for the private sector. To implement some of these recommendations, the report includes legislative language that could be adopted by Congress, in the next National Defense Authorization Act (NDAA), as a vehicle for enactment.

Below is a high-level overview of the CSC and some of the key recommendations from the Report. While the recommendations are expansive, this overview focuses on the potential impact on the private sector, especially owners and operators of critical infrastructure. If the Report's recommendations are adopted, industry will face new regulations and potential liabilities.

Authors

Megan L. Brown
Partner
202.719.7579
mbrown@wiley.law

Jon W. Burd
Partner
202.719.7172
jburd@wiley.law

Michael L. Diakiwski
Associate
202.719.4081
mdiakiwski@wiley.law

Kathleen E. Scott
Partner
202.719.7577
kscott@wiley.law

Practice Areas

Government Contracts

Privacy, Cyber & Data Governance

White Collar Defense & Government Investigations

What is the CSC? The Commission was established by Section 1652 of the 2019 NDAA, with a charge of "develop[ing] a consensus on a strategic approach to defending the United States in cyberspace against cyber attacks of significant consequences." The CSC is co-chaired by Senator Angus King (I-ME) and Representative Mike Gallagher (R-WI). Other Commission members include senior leaders from the Office of the Direction of National Intelligence (ODNI), Department Homeland Security (DHS), the Federal Bureau of Investigation (FBI), and the Department of Defense (DOD), as well as additional members selected by Congress. The CSC was inspired by President Dwight D. Eisenhower's 1953 Project Solarium which tasked different teams with developing strategic approaches to counter the Soviet Union during the Cold War and resulted in the adoption of a blended approach. The 2020 NDAA set a deadline for the delivery of CSC's recommendations for April 30, 2020. Leading up to the March 11 release of the Report, Commissioners participated in various rollout events to preview the major contours of their recommendations and CSC staff convened with various stakeholder groups.

Select Recommendations for the Private Sector. The Report contains dozens of recommendations spread across the following six core pillars:

1. Reform the U.S. Government's Structure and Organization for Cyberspace
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
6. Preserve and Employ the Military Instrument of Power

Although the pillars will have broad impacts—ranging from the military's cyber posture, international cooperation, global standards setting, and attribution, to election security—pillars 4 and 5 will likely have the most direct impact on private sector entities.

Several notable recommendations include:

- 4.1: ***Congress should establish and fund a National Cybersecurity Certification and Labeling Authority empowered to establish and manage a program for voluntary security certifications and labeling of information and communications technology products.***
- 4.2: ***Congress should pass a law establishing that final goods assemblers of software, hardware, and firmware are liable for damages from incidents that exploit known and unpatched vulnerabilities***.
- 4.3: ***Congress should establish a Bureau of Cyber Statistics charged with collecting and providing statistical data on cybersecurity and the cyber ecosystem to inform policymaking and government programs.***

- 4.4: ***Congress should resource and direct the Department of Homeland Security to resource a federally funded research and development center to work with state-level regulators in developing certifications for cybersecurity insurance products.***
- 4.4.3: ***Incentivize Information Technology Security through Federal Acquisition Regulations and Federal Information Security Management Act Authorities***
- 4.5: ***The National Cybersecurity Certification and Labeling Authority should develop a cloud security certification, in consultation with the National Institute of Standards and Technology, the Office of Management and Budget, and DHS.***
- 4.6: ***Congress should direct the U.S. government to develop and implement an industrial base strategy for information and communications technology to ensure trusted supply chains and the availability of critical information and communications technologies.***
- 4.7: ***Congress should pass a national data security and privacy protection law establishing and standardizing requirements for the collection, retention, and sharing of user data***.
- 4.7.1: ***Pass a national breach notification law.***
- 5.1: ***Congress should codify the concept of "systemically important critical infrastructure," whereby entities responsible for systems and assets that underpin national critical functions are ensured the full support of the U.S. government and shoulder additional security requirements consistent with their unique status and importance.***

Key Takeaways for the Private Sector. These recommendations, and others, would have a widespread impact on the private sector, touching issues that include privacy, breach notification, and supply chain security, among others. For example, Under 4.7, the Federal Trade Commission (FTC) would be given "a clear mandate" to enforce standards of a national data security and privacy protection law, with civil penalties. And under 4.2, the FTC would establish a regulation mandating transparency from final goods assemblers of software, hardware, and firmware.

These recommendations, if adopted, would also impact government contractors and federal procurement efforts. For example, the Report states that "[w]ithin five years the executive branch should consider updating federal procurement regulations and guidelines, including the Federal Acquisition Regulations, to require National Cybersecurity Certification and Labeling Authority certifications and labeling for certain information technology products and services procured by the federal government." The Report also stresses the interplay between contracting requirements and broader adoption of security practices, "the U.S. government is in a powerful position to help develop and generate more sustainable requirements for cybersecurity best practices, as requirements placed on government contractors can become de facto industry standards. Requiring vendors to adhere to standards when doing business with the federal government will compel them to produce product or service offerings that meet those standards, potentially making those more secure offerings available to the broader public."

Other recommendations in the Report are aimed at better integration and cooperation between the federal government and private sector to share information and intelligence, and address emerging threats and/or catastrophic cyber attacks. In particular, recommendations expand the authority and role of DHS' Cybersecurity and Infrastructure Security Agency (CISA), as well as other Sector Specific Agencies. One of the CSC's desired end states includes "public-private partnerships based on a shared situational awareness, combined action, and full support of the U.S. government in defense of the private sector."

While the Report covers large swaths of the economy, it focuses on several critical industries in particular. For example, the Report states that "given the cascading risks that will accompany widespread 5G deployment, the U.S. government has a responsibility to set clear cybersecurity standards in the marketplace," and the Information and Communications Technology (ICT) supply chain is a topic of key recommendations.

Private sector entities should be aware that federal agencies and Congress are taking a much more aggressive posture to cyber threats. This Report is a prime example, and industry should monitor whether these recommendations gain traction or are adopted. While the Report builds upon ongoing efforts, it takes a much larger step by enhancing roles and obligations for the private sector and actors in the economy—by going beyond "strategy building" to identifying and prescribing actions to be taken.

For years, Wiley attorneys have advised clients across the spectrum of emerging data security and privacy laws, covering requirements in the health care, telecommunications, government contracting, and financial services industries (as well as vendors to these industries), and the several statutes administered by the Federal Trade Commission (FTC). We are involved at the National Institute of Standards and Technology (NIST), shaping privacy engineering, cybersecurity, and Internet of Things (IoT) best practices. We also are working on key national security issues raised by data access and governance, particularly by foreign actors and investors.