wiley

ARTICLE

Insight: Will This Year's NDAA Have Cyber Surprises?

Bloomberg Law
May 4, 2020

Several recommendations from the Cyberspace Solarium Commission report could possibly be included in the National Defense Authorization Act. Wiley Rein LLP's Megan Brown says the report should be scrutinized due to the implications of several of the report's recommendations for the private sector.

The Cyberspace Solarium Commission report offers over 80 recommendations and dozens of legislative proposals on cybersecurity. As policymakers review it, questions are mounting about the process to implement them.

Some recommendations seem likely candidates for inclusion in the National Defense Authorization Act (NDAA), one of the few pieces of "must pass" legislation every year, but this may provide little opportunity for input on new obligations.

The NDAA has become a vehicle to regulate private sector activity. Commissioners and staff of the Solarium Commission made clear that many of its recommendations would be targeted for inclusion in the NDAA. Despite the Covid-19 pandemic, the fiscal year 2021 NDAA is moving and it is likely to contain—for better and worse—obligations for the private sector.

But, the process to draft the NDAA is not as transparent as other legislation and may not leave time for input, particularly given the inability to hold hearings and conduct in-person meetings during the pandemic.

Authors

Megan L. Brown
Partner
202.719.7579
mbrown@wiley.law

Practice Areas

Privacy, Cyber & Data Governance
Telecom, Media & Technology

The report has six relatively uncontroversial calls for specific action in the FY2021 NDAA. It says that Congress should direct the Department of Defense (DoD) to:

1. assess the force structure of the U.S. Cyber Command's Cyber Mission Force;

2. address U.S. Cyber Command as a major force program category in its budget justification;

3."conduct a cybersecurity vulnerability assessment" for nuclear command and control;

4. assess a military cyber reserve;

5. and assess the current Pathfinder initiative, including expanding private collaboration on critical infrastructure.

It also calls for the National Security Agency to "assess the threats and risks posed by quantum technologies to national security systems and develop a plan to secure those systems."

The more interesting question is what else might be put into the NDAA from the Solarium Commission report.

Past NDAAs Have Addressed ICT and Cybersecurity of the Private Sector

The FY2019 NDAA affected the private sector, for example in Section 889, implementation of which is still rolling out. In August and December 2019, the Federal Acquisition Regulation (FAR) Council released rules to implement Section 889(a)(1)(A), which prohibits agencies from procuring "any equipment, system, or service that uses covered telecommunications equipment or services" from certain Chinese telecom companies.

There is angst in the private sector about the breadth of Section 889's broader prohibition on government contracting with any companies that "use" telecom equipment or services from Huawei or ZTE, because it could encompass uses unrelated to the performance of government contracts.

The FY2020 NDAA affected the private sector, particularly on information and communications technology supply chain. For example, it added Huawei to the Bureau of Industry and Security's Entity List to prohibit exports of U.S. goods, software, and technology to Huawei.

Solarium Commission Report Targets Government and Private Sector

In addition to recommendations explicitly intended for inclusion in the FY2021 NDAA, the Solarium Commission report offers a host of legal and policy recommendations that signal a fundamental shift in U.S. cybersecurity policy. It calls for the government to "explore legislation, regulation, executive action, and public- as well as private-sector investments" to improve the nation's cybersecurity posture.

The report repeatedly uses the phrase "Congress should pass a law" and offers proposals that would affect the private sector such as:

- Seeming to endorse the Cybersecurity Maturity Model Certification (CMMC) regime rolled out by the DoD, which could require contractors to obtain a third-party cybersecurity certification.
- Recommending a National Cybersecurity Certification and Labeling Authority to establish voluntary standards for information and communications technology products.
- Recommending amendments to Sarbanes-Oxley to require companies to make more disclosures and conduct third party review of internal cyber controls.
- Recommending that Congress 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.

The Solarium Commission calls for expanding the reach and authority of government in several areas, including major investments in the Cybersecurity and Infrastructure Security Agency (CISA) at Department of Homeland Secuity. The report envisions a new Integrated cyber center within the CISA, and it calls for a new Bureau of Cyber Statistics to collect and provide statistical data on cybersecurity.

An invigorated Supply Chain and Counterintelligence Risk Management Task Force in the Office of the Director of National Intelligence will build on the FY2020 NDAA and expand work with the private sector to "improve information sharing on supply chain risk." It envisions a new approach to "systemically important critical infrastructure" with new obligations. And, it calls for expanded subpoena authority across government, which would result in more subpoenas reaching the private sector.

These and other efforts will increase burdens for the private sector.

The Solarium Commission report also offers recommendations that focus on the military and Defense Industrial Base (DIB), but which will affect the private sector. For example:

- Requiring DIB participation in a threat intelligence sharing program will impose additional burdens on the private sector;
- Requiring threat hunting on DIB networks would require companies that have contracts with the DoD to create a mechanism for government threat hunting, raising privacy and access issues; and
- Addressing risks to national security posed by quantum computing will bring the government into private sector innovation, as the government develops its views on risks and how to "secure" quantum.

Due to their implications for the private sector, these recommendations should be scrutinized. But putting broad new regulations, authorities, or programs into the NDAA may limit the opportunity for input.

The Senate Committee on Armed Services, Subcommittee on Cybersecurity postponed its planned hearing on the Cyberspace Solarium Commission report, which would have shed some light on priorities for the FY2021 NDAA. Congressional staff and the private sector may want to insist on hearings and opportunity for comment.

Private companies—in and outside of the DIB—should review the recommendations of the Cyberspace Solarium Commission to see how they might affect their business, operations, and relationship with government. Policymakers that are not deep in the NDAA may welcome input about the burdens of various proposals. When opportunities for input arise, companies should share their perspectives.

This column does not necessarily reflect the opinion of The Bureau of National Affairs, Inc. or its owners.