wiley

NEWSLETTER

# Update on NDAA FY18 Cyber Provisions

February 2018

*Government Contracts Issue Update*

The FY18 NDAA encompasses a broad range of cybersecurity issues that play an important role in DOD's priorities and budget. For industry, the Department's cyber plans offer both opportunity and peril. This article highlights several of the key cyber provisions and initiatives that will affect industry.

Notably, we expect that DOD will work closely with the Department of Homeland Security (DHS) on a number of key cyber issues, including DOD's requirement to rid certain defense and homeland security systems of any telecommunications equipment and services produced by Huawei, ZTE, or any other telecommunications equipment or services produced or provided by an entity owned, controlled by, or otherwise connected to the Chinese or Russian government. Section 1656 of the NDAA, which restricts the use of such equipment and services in certain defense and homeland security infrastructure, was referenced by DHS at a recent Cybersecurity Working Group (CSWG) meeting as an area in which DHS will be active. DHS will also play a role in drafting a comprehensive cyber posture review, which will set out the near-term policy and strategy for cyber deterrence. More generally, we also expect increasing attention to cybersecurity and cyber compliance throughout federal procurements, as contractors must begin to comply with the requirements in DFARS 252.204-7012 and NIST SP 800-171, and as congressional proposals, such as the Warner-Gardner IoT bill, percolate.

The NDAA also reflects a focus on continued government investment in cyber capabilities and resources. Section 1078, for example, establishes a Technology Modernization Fund and Board designed to improve and replace through acquisitions existing and obsolete Federal IT and cybersecurity systems. Continued funding for

## Authors

Megan L. Brown
Partner
202.719.7579
mbrown@wiley.law

## Practice Areas

Government Contracts
Privacy, Cyber & Data Governance

cybersecurity research and development contracts and cooperative agreements, as well as funding for cybersecurity education and scholarships, is also provided. The NDAA also is notable for ***prohibiting*** the Government from acquiring certain products and services. As noted above, pursuant to Section 1656, certain DOD systems must not include telecommunications equipment or services produced by Huawei, ZTE, or any company owned, controlled by, or "otherwise connected to" the Chinese or Russian government. Similarly, Section 1634 permanently bans Kaspersky Lab's products from use by any federal agency.

The NDAA also impacts private investment. We expect cyber to play an increasingly important role in the Committee on Foreign Investment in the United States (CFIUS). Cybersecurity and IT acquisitions have come under close scrutiny by CFIUS in recent years, particularly transactions having any nexus to China or Chinese State Owned Entities (SOE). Moreover, in transactions across a spectrum of industries, CFIUS continues to pay close attention to the data privacy, information access, and cybersecurity implications of those transactions. The NDAA, Section 1069, builds on this trend by calling on DOD, with other agencies, to develop a plan and recommendation to improve the effectiveness of CFIUS, while focusing on the "major vulnerabilities of the defense industrial base pertaining to foreign investment, including in the areas of cybersecurity [and] reliance on foreign suppliers in the defense supply chain."

Finally, Section 1633 of the NDAA calls on the President to develop a national policy relating to cyberspace, cybersecurity, and cyber warfare; a report on the policy is to be submitted to the appropriate congressional committees. This policy will address the instruments of national power available to deter or respond to cyber attacks, available response options and capabilities that may impose costs on foreign powers, and enhanced attribution and offensive cyber capabilities.