wiley

ALERT

Important Cyber Provisions Now Law Under the 2019 NDAA

August 13, 2018

The John S. McCain National Defense Authorization Act for Fiscal Year 2019 (NDAA or the Act) (H.R. 5515) was signed into law on August 13, 2018. The appropriations law authorizes a $716 billion national defense budget and includes wide-ranging provisions on cybersecurity, touching everything from enhancing the military's ability to respond to cyber attacks to protecting the IT supply chain and encouraging greater public-private collaboration. Below, we outline key elements of the law, which will impact how private industry engages with the U.S. Department of Defense (DOD) on cybersecurity issues.

Wiley Rein further addresses other important aspects of the 2019 NDAA, including sections reforming the Committee on Foreign Investment in the United States (CFIUS) and provisions impacting government contractors.

Key Takeaways for the Private Sector

- The Act establishes a more aggressive posture on U.S. cybersecurity policy, stating that "all instruments of national power" will be used to defend, deter, and respond to significant cyber threats.
- The NDAA exemplifies a government-wide trend of increased expectations on the private sector, for greater collaboration and scrutiny of security in IT products and services; but this is coupled with enhanced government assistance and commitments to defend U.S. networks, systems, and critical infrastructure. Further, the law requires more thorough collaboration between civil authorities (such as the U.S. Department of Homeland Security) and the military, in

Authors

Megan L. Brown
Partner
202.719.7579
mbrown@wiley.law

Jon W. Burd
Partner
202.719.7172
jburd@wiley.law

Practice Areas

Privacy, Cyber & Data Governance

managing and responding to cyber threats and incidents.

- The law prohibits federal government agencies from using or procuring certain covered technologies, with some exceptions.
- Several provisions require consultation with and reference frameworks produced by the National Institute of Standards and Technology (NIST). NIST's cybersecurity frameworks, standards, and guidelines are typically drafted for use by the federal government. Increasingly, however, these documents are cited in pending legislation and by sector-specific agencies for use by industry.
- Certain DOD contractors, vendors, and suppliers of operational technology, cybersecurity, industrial control systems, and weapons systems developed for DOD must now make supply chain disclosures related to foreign ownership or obligations. The Secretary of Defense has expanded authority to draft regulations and mitigate supply chain risk.
- Related to information technology, cybersecurity, systems engineering, and other technical services, the NDAA outlines that the cost-savings principle known as the "lowest price technically acceptable" shall be avoided in circumstances that would deny the government the benefits of cost and technical trade-offs in the source selection process. This is a recognition that network, system, and device security concerns may outweigh value and cost considerations in procurements.
- Under the NDAA's CFIUS reform act, certain investments in critical technology, critical infrastructure companies, and companies that maintain or collect sensitive personal data of U.S. citizens may be subject to CFIUS jurisdiction.

Establishing U.S. Policies on Cyberspace, Cybersecurity, Cyber Warfare, and Cyber Deterrence

Section 1636 outlines the "Policy of the United States on cyberspace, cybersecurity, cyber warfare, and cyber deterrence." The policy signifies a more aggressive posture, bringing greater resources to bear in preventing, deterring, and responding to cyber threats – including through offensive cyber operations. "[T]he United States should employ all instruments of national power, including the use of offensive cyber capabilities, to deter if possible, and respond to when necessary, all cyber attacks or other malicious cyber activities of foreign powers that target United States interests[.]"

This includes cyber threats to private sector systems, covering activities which "significantly disrupt the normal functioning of United States democratic society or government (including attacks against critical infrastructure that could damage systems used to provide key services to the public or government)."

The section calls for the development of a plan for "response options to address the full range of potential cyber attacks on United States interests that could be conducted by potential adversaries[.]" Within 180 days of the law's passage, classified and unclassified reports on U.S. cyber policy are to be delivered to relevant congressional committees. Among other things, this report would cover:

- "Information relating to the Administration's plans, including specific planned actions, regulations, and legislative action required [for]:

- (i) advancing technologies in attribution, inherently secure technology, and artificial intelligence society-wide;
- (ii) improving cybersecurity in and cooperation with the private sector; [and]
- (iii) improving international cybersecurity cooperation[.]"

Establishing the 'Cyberspace Solarium Commission'

Aligned with the general policy pronouncements outlined above, Section 1652 allocates $4 million to establish "a commission to develop a consensus on a strategic approach to defending the United States in cyberspace against cyber attacks of significant consequences." The Cyberspace Solarium Commission would be formed within 45 days of enactment. Members include senior leaders from the Office of the Direction of National Intelligence, Homeland Security, the Federal Bureau of Investigation, and DOD, as well as 10 additional members selected by Congress. The Commission would be able to hold hearings, request information, and subpoena witnesses. Among others, core objectives are to:

- Develop a consensus on a strategic approach to defending the United States in cyberspace.
- Weigh the costs and benefits, and evaluate the means, for executing various strategic options, including for the political system, the national security industrial sector, and the innovation base. Options to be assessed include deterrence, norms-based regimes, and active disruption of adversary attacks through persistent engagement.
- Review and make determinations on norms-based regimes and how the United States should enforce such norms.
- Review adversarial strategies and intentions.
- Evaluate the effectiveness of the current national cyber policy and consider possible structures and authorities that need to be established, revised, or augmented within the federal government.

A final report with the Commission's findings is due September 1, 2019.

Prohibition on Certain Telecommunications Equipment

Section 889 prohibits the use of federal funds to acquire "covered telecommunications equipment or services." This term is defined generally to include: telecommunications equipment produced by Huawei Technologies Company or ZTE Corporation (or any subsidiary or affiliate of such entities); certain uses of video surveillance technology and equipment produced by Hytera Communications Corporation, Hangzhou Hikvision Digital Technology Company, or Dahua Technology Company (or any subsidiary or affiliate of such entities); telecommunications of video surveillance services provided by such entities or using such equipment; and such equipment and services that the Secretary of Defense "reasonably believes to be an entity owned or controlled by, or otherwise connected to, the government of a covered foreign country."

Under Section 889 executive agency heads may not "procure or obtain or extend or renew a contract to procure or obtain any equipment, system, or service that uses covered telecommunications equipment or services as a substantial or essential component of any system, or as critical technology as part of any system." This prohibition is effective August 13, 2019.

The law further prohibits executive agency heads from "enter[ing] into a contract (or extend[ing] or renew[ing] a contract) with an entity that uses any equipment, system, or service that uses covered telecommunications equipment or services as a substantial or essential component of any system, or as critical technology as part of any system." This prohibition is effective August 13, 2020.

Section 889 also prohibits the use of federal loan or grant funds to procure or obtain covered telecommunications equipment or services. This prohibition is effective August 13, 2020. In implementing this prohibition certain agency heads—including the Chair of the Federal Communications Commission and Secretaries of Commerce and Homeland Security, among others—"shall prioritize available funding and technical support to assist affected businesses, institutions and organizations as is reasonably necessary for those affected entities to transition from covered communications equipment and services, to procure replacement equipment and services, and to ensure that communications service to users and customers is sustained."

Certain exceptions apply for entities that "provide a service that connects to the facilities of a third-party, such as backhaul, roaming, or interconnection arrangements; or cover telecommunications equipment that cannot route or redirect user data traffic or permit visibility into any user data or packets that such equipment transmits or otherwise handles." Further one-time waivers may be available to companies, if approved by an agency.

Mitigating Cybersecurity and IT Supply Chain Risks

Supply chain IT risk is addressed in Section 1655. Subject to forthcoming regulations, DOD "may not use a product, service, or system procured or acquired ... relating to information or operational technology, cybersecurity, an industrial control system, or weapons system," unless the certain information is disclosed to the Secretary of Defense, including:

- Whether an organization or person has allowed, or is under an obligation to allow, a foreign government to review the code of a noncommercial product, system, or service developed for DOD. This provision covers conduct up to five years before the enactment of the NDAA.
- Whether an organization or person has allowed, or is under an obligation to allow, a foreign government or person from the countries listed in Section 1654 to review the source code of a product, system, or service that DOD is using *or intends to use*. This provision covers conduct up to five years before the enactment of the NDAA.
- Whether a person holds or has sought a license pursuant to Export Administration Regulations under Subchapter C of Chapter VII of Title 15, Code of Federal Regulations, the International Traffic in Arms Regulations under Subchapter M of Chapter I of Title 22, Code of Federal Regulations, or successor

regulations, for information technology products, components, software, or services that contain code custom developed for the noncommercial product, system, or service the Department is using or intends to use.

The Secretary of Defense is directed to issue regulations implementing these supply chain disclosure requirements. Within a year, a registry is to be created to collect and maintain information disclosed, which can be made available to any agency conducting a procurement pursuant to the Federal Acquisition Regulations or the Defense Federal Acquisition Regulations.

If the Secretary determines such disclosures reveal "a risk to the national security infrastructure or data of the United States, or any national security system under the control of the Department," the Secretary shall take appropriate mitigation actions, including "conditioning any agreement for the use, procurement, or acquisition of the product, system, or service on the inclusion of enforceable conditions or requirements that would mitigate such risks." Within two years of the NDAA's passage, DOD shall develop a third-party testing standard "acceptable for commercial off the shelf (COTS) products, systems, or services to use when dealing with foreign governments."

Further, Section 881 contains a provision that permanently extends the authority provided in Section 806 of the Ike Skelton National Defense Authorization Act for Fiscal Year 2011 (Public Law 111–383) regarding the management of supply chain risk, and would clarify the Secretary of Defense's ability to make determinations under that authority to apply throughout DOD.

Increased Collaboration between Civil Authorities and the Private Sector

Several sections encourage greater collaboration between DOD, civil authorities, and the private sector. For example, Section 1650 establishes a pilot program, coordinated by the Secretaries of DOD and Homeland Security. Technical cybersecurity professionals from DOD will be detailed to the Department of Homeland Security, including the National Cybersecurity and Communications Integration Center (NCCIC), in order to "enhance cybersecurity and resilience of critical infrastructure."

Section 1648 outlines U.S. Cyber Command involvement in "tier 1 exercise[s]" including coordination with "the Department of Homeland Security, the Federal Bureau of Investigation, and elements across Federal and State governments and the private sector." And Section 1649 establishes another pilot program to "assess defense critical infrastructure vulnerabilities and interdependencies to improve military resiliency" and "foster collaboration and learning between and among departments and agencies of the Federal Government, State and local governments, and private entities responsible for critical infrastructure," among other things. The program will model cyber attacks on critical infrastructure in order to identify and develop means of improving DOD responses to requests for support to civil authorities.

Software & Cloud Security Related to Critical Systems

Section 1657 of the Act calls for a study of the costs, benefits, technical merits, and other merits of the following technologies related to vulnerability assessments of nuclear systems, a critical subset of conventional power projection capabilities, and cyber command and control. This study will cover:

- Technology acquired, developed, and used by Combat Support Agencies of the DOD to discover flaws and weaknesses in software code.
- Cloud-based software fuzzing-as-a-service to continuously test the security of DOD software repositories at large scale.
- Formal programming and protocol language for software code development and other methods and tools developed under various programs.
- The binary analysis and symbolic execution software security tools developed under the Defense Advanced Research Projects Agency (DARPA) program.
- Any other advanced or immature technologies with respect to which DOD determines there is particular potential for application to the vulnerability assessment and remediation of the systems.

Designation of a DOD Official for Cyber Integration and Industrial Control Systems

Section 1643 states that, within 180 days of enactment, one official will be designated to be responsible for matters relating to integrating cybersecurity and industrial control systems for DOD. That official shall be responsible for "developing Department-wide certification standards for integration of industrial control systems and taking into consideration frameworks set forth by the NIST for the cybersecurity of such systems."

Investments in Critical Technology, Critical Infrastructure, and Sensitive Personal Data Companies May be Subject to CFIUS Review

As outlined in Wiley Rein's review of CFIUS reforms, certain investments in critical technology and critical infrastructure companies and companies that maintain or collect sensitive personal data of U.S. citizens will be subject to CFIUS jurisdiction if the investment could afford a foreign person access to material nonpublic technical information, board membership or observer rights or the right to nominate a board member, or certain substantive decision-making involvement (other than through voting of shares). Indirect investments by a foreign person through an investment fund that affords the foreign person membership as a limited partner on an advisory board or committee of the fund are excluded from this provision as long as certain criteria are met.

Other Noteworthy Cyber Provisions

Authority to Conduct Military Activities in Cyberspace. Section 1632 affirms the authority of the Secretary of Defense to direct "military cyber activities or operations in cyberspace, including clandestine military activities or operations in cyberspace[.]" These clandestine activities or operations will be considered "traditional military activity," as defined in the National Security Act of 1947.

Avoidance of the "Lowest Price Technically Acceptable" Selection Criteria with Certain Tech. Section 880 states, "the use of lowest price technically acceptable source selection criteria shall be avoided in the case of a procurement that is predominately for the acquisition of information technology services, cybersecurity services, systems engineering and technical assistance services, advanced electronic testing, audit or audit readiness services, health care services and records, telecommunications devices and services, or other knowledge-based professional services[.]" The House Report notes that the U.S. Government Accountability Office is expected to develop a methodological approach that will provide insight into the extent to which lowest price technically acceptable source selection criteria are used by executive agencies.

Applying DHS Binding Operational Directives. Section 1645 directs the Secretary to implement Binding Operational Directive 18-01 on email and Internet security issued by the Secretary of Homeland Security. Further, regarding future DHS cybersecurity Directives, the CIO of DOD shall notify relevant committees "whether [DOD] will comply with the Directive or how [it] plans to meet or exceed the security objectives of the Directive."

DOD Reporting Requirements on Cyber Breaches and Loss of PII and CUI. In the case of "a significant loss of personally identifiable information [PII] [or] controlled unclassified information [CUI] by a cleared defense contractor," the Secretary "shall promptly submit to the congressional defense committees notice in writing of such loss." Whether or how this provision will impact notification requirements for contractors and vendors remains to be seen.

Increased Assistance for Small Manufacturers & Universities. In consultation with NIST, DOD shall take actions to "enhance awareness of cybersecurity threats among small manufacturers and universities" working on DOD programs and activities. This is aimed at enhancing security in the Defense Industrial supply chain. Outreach activities include training, courses, and self-certification to help these parties improve cybersecurity.

Transferring the SHARKSEER Cybersecurity Program. The SHARKSEER cybersecurity program, which identifies and mitigates Zero Day malware and Advanced Persistent Threats using commercial technology, is to be transferred from the National Security Agency to the Defense Information Systems Agency.

Identification of Countries Posing Risks to U.S. Cybersecurity. Within 180 days of enactment, the Secretary of Defense "shall create a list of countries that pose a risk to the cybersecurity of United States defense and national security systems and infrastructure. Such list shall reflect the level of threat posed by each country included on such list." Another section, grants authority to "disrupt, defeat, and deter cyber attacks" originating from the Russian Federation, People's Republic of China, Democratic People's Republic of Korea, or Islamic Republic of Iran, including attempts in influence American elections and democratic processes.

Promoting Cybersecurity Education. DOD has greater authority for cyber-related grants and scholarships and the Secretary will establish a Cyber Institute. Further, within 240 days a report shall be submitted to congressional committees on the feasibility of establishing a Cybersecurity Apprentice Program to support on-the-job training for certain cybersecurity positions and facilitate the acquisition of cybersecurity certifications.