wiley

ALERT

Section 889 of the 2019 NDAA is Looming, Creating Compliance Challenges Across the Economy, Including for Tech

June 12, 2020

The National Defense Authorization Act (NDAA) is annual must-pass legislation that has gradually taken on more importance beyond the Defense Industrial Base. While this is true of the 2021 NDAA currently being negotiated, the 2019 NDAA still looms large as companies start to appreciate its breadth in advance of an August 13, 2020 compliance deadline for which regulations have not yet been made public. These issues were in the news this week and will continue to be as we move forward.

In the government's efforts to significantly reduce reliance on what it perceives to be problematic Chinese-made equipment, private sector companies that have never done business with the federal government and may never have heard of the NDAA are now facing hard questions about their operations and IT networks, as well as their subsidiaries' and affiliates' use of covered equipment, from customers who do business with the government or who plan to. At the same time, companies that do, or want to do, business with the federal government, are cataloging their own systems and their partners' systems—while also wondering how far they have to go and how they can ever be sure they are compliant.

Section 889 of FY2019 NDAA is Creating Headaches

Section 889 was intended to ensure that federal government procurements did not include "covered telecommunication equipment or services" produced by Huawei, ZTE, Hytera, Hikvision, and Dahua or their subsidiaries as a "substantial or essential component of any system, or as critical technology as part of any system."

Authors

Megan L. Brown
Partner
202.719.7579
mbrown@wiley.law

Nova J. Daly
Senior Public Policy Advisor
202.719.3282
ndaly@wiley.law

Tracye Winfrey Howard
Partner
202.719.7452
twhoward@wiley.law

Brandon J. Moss
Partner
202.719.7554
bmoss@wiley.law

Practice Areas

Government Contracts

National Security

Telecom, Media & Technology

White Collar Defense & Government Investigations

Section 889 has two key parts, both of which restrict U.S. spending and affect contractors and their supply chains. Part A, Section 889(a)(1)(A), prohibits the federal government from procuring or obtaining, or extending or renewing 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." On August 13, 2019, Federal Acquisition Regulation (FAR) clauses 52.204-24 and 52.204-25 went into effect to implement that part. Notably, consistent with the statute, the clauses do not prohibit contractors from providing "a service that connects to the facilities of a third-party, such as backhaul, roaming, or interconnection arrangements" or "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."

While many contractors scrambled to assess the supply chains of products and services covered by Part A, it is Part B of the law, Section 889(a)(1)(B) that is really causing headaches as the August 13, 2020 deadline for compliance with that Part looms.

Part B is drafted far more broadly, purporting to prohibit the federal government from entering into or extending or renewing contracts with any entity that "uses any equipment, system, or service that uses covered telecommunication equipment or services as a substantial or essential component of any system, or as critical technology as part of any system." This is an effective debarment from all government contracting of companies that use systems that use covered telecom equipment or services. Notably, the statute also requires that the use be "as a substantial or essential component," but that limitation remains undefined.

The regulations implementing Part B have not been released, causing great angst for companies who are trying to assess their ability to do business with the government – or sell to those who do business with the government – going forward. As recently reported in the press, business groups have been lobbying for changes in the statute or a delay in the compliance deadline: "If part B is implemented as written, many businesses with international and domestic operations will be forced to halt their work providing key products and services to agencies," according to several trade associations. An influential Senator tweeted his opposition to regulatory relief.

Of course, a lot can happen between now and August 13, 2020, including possible waivers, class deviations, or alternative regulatory approaches. But companies should be considering their vendors, suppliers, and infrastructure to evaluate how the plain terms Part B of section 889 would apply to them, either directly as a contractor or indirectly as a supplier or vendor to a government contractor. They should also be carefully documenting their efforts at analysis and outreach so that there is a clear record to support their good-faith due diligence, should that become an issue in a False Claims Act or contract action down the road.

FY2021 NDAA is Racing Ahead, with Likely Impacts on Supply Chains, 5G, Cyber, AI, and More

While companies grapple with Section 889, we are already looking ahead to the next NDAA.

On June 11, 2020, the Senate Armed Services Committee released its summary of the Fiscal Year 2021 NDAA. As expected, it contains several provisions of interest in the areas of cyber and 5G. This is consistent with recent Department of Defense (DoD) planning activities focused on 5G, and on past congressional directions, as in the 2019 NDAA, to restrict the access of certain Chinese telecom companies to DoD networks. As described in the summary, the Senate version of the FY2021 NDAA doubles down on that approach, with even more emphasis on security risks from China—though Russia gets stern treatment as well. The Senate bill envisions an important role for DoD in 5G, and contains recommendations from the recent Cyberspace Solarium Report, which we described here, including some that will increase regulatory expectations of contractors and will involve DoD in artificial intelligence, quantum, 5G, and more.

The draft bill would do a variety of things, from increasing expectations for software provided to the government, to mandating participation in information-sharing by certain contractors. It aims to increase scrutiny and resiliency of the United States' manufacturing and defense industrial base and supply chain and to take steps to encourage re-shoring and building up U.S. domestic capacity in a variety of materials and technology sectors, like microelectronics, rare earth minerals, medical devices, personal protective equipment, and pharmaceutical ingredients.

This draft bill portends a more ambitious DoD role in 5G and other emerging technology, which are already being looked at by the Department of Commerce, Department of Homeland Security, the Federal Communications Commission, and other agencies for possible regulation, export control, and research and development funding. Wiley will continue to monitor developments and provide additional updates on this topic as events unfold.