wiley

ALERT

Recent Legislation Could Ban Federal IT Purchases of Certain Chinese Equipment

March 27, 2013

On Thursday, March 21, Congress passed a law that included a provision that would ban certain federal government purchases of information technology products made by firms that the Chinese government owns, directs or subsidizes. The provision, which could affect U.S. and foreign suppliers and producers, was included as Section 516 in H.R. 933, the continuing resolution (CR) bill which funds the federal government for the next six months. The President signed the bill into law on Wednesday, March 26.

The ban in Section 516(b) prohibits federal government acquisitions of information technology systems if they were "produced, manufactured or assembled" by an entity that is "owned, directed or subsidized" by the People's Republic of China (PRC). Importantly, the provision does not define what constitutes ownership, direction or subsidization. This creates a notable degree of uncertainty as to the scope of the ban because defining these terms will be left up to the Administration. The Chinese government regularly subsidizes their domestic industries and state-owned enterprises (SOEs). In its latest five-year plan, China identified information technology as one of seven "strategic emerging industries" which are critical to its next phase of development and which will receive heavy government investment. Furthermore, so long as it is directed or subsidized by the PRC, an entity need not even be owned by Chinese nationals or located in China for this section to apply. This has implications not only for Chinese companies, but also for U.S. companies that procure Chinese products and sell to the U.S. government.

In any potential sales to the U.S. government, companies may need to examine closely whether any of the entities in their production or manufacturing chain could have any relevant ties to the Chinese

Authors

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

Practice Areas

International Trade
Privacy, Cyber & Data Governance
Telecom, Media & Technology

government. Thus, the law may bar the acquisition of information technology not only from certain Chinese firms, but also from American companies seeking to sell information technology products to the federal government if they utilize products that fall within the legislation's mandate. Installers or producers of computers, telecommunications systems or any other information technology may also be impacted. Thus, how the Administration chooses to define the terms of the provision will have great effect on its application. In either case, the affected government agencies seeking to procure information technology will likely increase their scrutiny of companies' manufacturing chains in order to determine compliance with the law.

Section 516(b) does, however, provide a limited national interest exception. The federal agencies affected by the law (*i.e.,* the U.S. Departments of Commerce and Justice, NASA and the National Science Foundation) may nonetheless acquire such information technology when the head of the agency: (1) consults with the Federal Bureau of Investigation or other appropriate federal entity and makes a cybersecurity assessment, (2) determines that an acquisition would be "in the national interest of the United States," and (3) reports that determination to the House and Senate Appropriations Committees. The complexity and high-level process for the exception indicates the rarity with which Congress intends it to be invoked.

This provision is a significant addition to a number of measures that the U.S. government has implemented in the last few months to enhance the nation's cybersecurity. The recently-released 2012 Annual Report on federal information security efforts found that Executive branch agencies' compliance with mandated information technology security programs dropped slightly in the last fiscal year, and identified key areas for focused improvement for the next fiscal year. Additionally, last month President Obama issued an Executive Order on Improving Critical Infrastructure Cybersecurity that requires improvement in government-to-private sector cyber threat sharing.

Wiley Rein closely tracks cybersecurity law and policy and engages Congress and the Administration in advising, interpreting and applying applicable cyber law and policy. Our cybersecurity team, which consists of former senior level Executive branch appointees and congressional staffers, is exceptionally placed to provide guidance on the latest critical information and intelligence related to cybersecurity law and policy and stands ready to work with companies to understand applicable provisions and to comply with relevant law.