Lowenstein Sandler

Global Trade & Policy

July 17, 2020

DOE's Recent RFI Specifies "Foreign Adversaries" – What Does it Mean?

By Doreen M. Edelman, Abbey E. Baker, and Christian C. Contardo

What You Need To Know:

- **Recent events emphasize the effect of the U.S.-China relationship on imports, exports, and foreign investment.**
- **Companies should consider looking closely at whether and how their products or services could be considered a national security concern in a variety of regulatory capacities, including foreign investment, export controls, and even real estate.**
- **Companies should also identify the beneficial owners of their customers and investors to better understand any potential U.S. government investigation of their business.**

Reflecting increasing U.S. government concern regarding Chinese access to U.S. critical technologies and critical infrastructure, *POWER* magazine recently reported on the Department of Energy's (DOE) publication of a Request for Information (RFI) to "identify and understand vulnerabilities in current energy industry practices." The RFI comes amid tense relations with China and, as illustrated by FBI Director Wray's recent public remarks on FBI counterintelligence investigations regarding China, could be an indication of increasing U.S. government scrutiny of legal Chinese investment across industries and sectors where U.S. national security might be implicated.

- Among the important aspects of the DOE publication, *POWER* notes that the DOE issued a definitive list identifying six foreign adversaries that it believes pose threats to the U.S. bulk power system (BPS): China, Cuba, Iran, North Korea, Russia, and Venezuela.
- *POWER* reports that the RFI also hints at possible next steps the federal government may take to execute the May 1, 2020 Executive Order 13920.
  - Declaring a national emergency over BPS threats, EO 13920 essentially seeks to ban the "acquisition, imports, transfers, or installation" of any risk-ridden BPS electric equipment in which a foreign adversary or a citizen of countries deemed adversaries has any interest, including "through an interest in a contract for the provision of the equipment."
  - The EO prohibits transactions covering pending and future deals for BPS equipment that have been designed, developed, manufactured, or supplied by vendors and individuals subject to the jurisdiction of a "foreign adversary."
- DOE also warns that China and Russia "have the capability and integrated plans necessary to launch cyber-attacks causing localized, disruptive effects on critical infrastructure—such as the disruption of a natural gas pipeline and electric infrastructure for days to weeks—in the U.S." It adds, "These near-peer foreign adversaries continue to map U.S. critical infrastructure with the long-term goal of being able to cause substantial damage."

- DOE suggests the two countries are actively "employing innovative combinations of traditional spying, economic espionage, and supply chain and cyber operations to gain access to critical infrastructure. They are also attempting to access our Nation's key supply chains at multiple points—from concept to design, manufacture, integration, deployment, and maintenance—by, among other things, inserting malware into important information technology networks and communications systems."
- Among questions the agency is asking energy sector asset owners and vendors to answer voluntarily by Aug. 7, 2020, are whether they conduct enterprise risk assessments on a periodic basis, and **whether they identify (and mitigate) foreign adversary ownership, control, and influence** with respect to "company and utility data, product development, and source code (including research partnerships)."
- The DOE publication follows recent public remarks by FBI Director Wray regarding the volume and breadth of its China counterintelligence investigations. According to news reporting, Wray stated that almost half of the FBI's nearly 5,000 active counterintelligence investigations involve China, with the bureau opening a new China-related counterintelligence case every 10 hours. As reported in *Nextgov*, and according to Wray:
  - **China is escalating improper and sometimes illegal activity in the wake of the coronavirus pandemic, using a mix of sophisticated cyber-intrusion techniques and the corruption of "trusted insiders"** to siphon America's intellectual property
  - China is employing economic espionage to **target the American aviation, robotics, agriculture, and health care sectors**—part of a broader plan to subvert American economic dominance that has resulted in a 1,300% increase in economic espionage cases linked to China over the past decade.
    - Wray said the American people are victims "of what amounts to Chinese theft on a scale so massive that it represents one of the largest transfers of wealth in human history" and poses a major national security threat.
  - "China often steals American intellectual property and then uses it to compete against the very American companies it victimized—in effect, cheating twice over. They're **targeting research on everything from military equipment to wind turbines to rice and corn seeds**."
    - "China is engaged in a whole-of-state effort to become the world's only superpower by any means necessary," Wray said. "The greatest long-term threat to our nation's information and intellectual property, and to our economic vitality, is the counterintelligence and economic espionage threat from China. It's a threat to our economic security—and by extension, to our national security."
  - China uses "a diverse range of sophisticated techniques," from cyber-intrusions to penetrate and steal trade secrets to the corruption and bribing of "trusted insiders."
  - China is making use of less overt forms of influence as well, such as its talent recruitment programs, wherein China attempts to "entice scientists to secretly bring our knowledge and innovation back to China." Wray pointed to scientist Jongjin Tan, a 36-year-old Chinese national and lawful permanent U.S. resident, as a clear example of this sort of influence. In November 2019, Tan pleaded guilty to stealing proprietary information worth more than $1 billion from his employer, **a U.S. petroleum company**. Tan was recruited by China after he joined China's Thousand Talents Program.

We advise U.S. companies to do the following:

- Ensure you are aware of the beneficial ownership of all of your investors, suppliers, and partners, as well as the access each has to data and technology, particularly if you are in an industry related to critical technology, critical infrastructure, or any area that could raise national security concerns.
- Diversify your supply chain to have alternatives to adversarial country suppliers. You never know when there will be a regulation or executive order requiring diversification, tariffs, or reporting with virtually no lead time.
- Understand which employees working in your organization are foreign nationals (by citizenship and country of birth), and know the roles they play and the data and technology to which they have access.
- Have sanctions and import and export policies with specific procedures in place, and ensure you are complying with government restrictions on technology transfers, whom you can do business with, and where you can do business.

Contacts

Please contact the listed attorneys for further information on the matters discussed herein.

DOREEN M. EDELMAN
Partner
Chair, Global Trade & Policy
T: 202.753.3808
dedelman@lowenstein.com

ABBEY E. BAKER
Counsel
T: 202.753.3806
abaker@lowenstein.com

CHRISTIAN C. CONTARDO
Associate
T: 202.753.3804
ccontardo@lowenstein.com