

DOE Requests Information to Secure the Bulk-Power System from “Foreign Adversaries”

20 July 2020

Developers and sponsors have a soon-ending opportunity to make their views known to the U.S. Department of Energy (“DOE”) on its recent [Request for Information](#) (“RFI”) “to understand the energy industry’s current practices to identify and mitigate vulnerabilities in the supply chain for components of the bulk-power system (BPS).” Comments responding to the RFI are due by August 7. Later this year, it is expected that DOE will issue proposed rules to regulate this area, and the RFI provides insight into features those rules are likely to contain.

Background: Uncertainty over Scope of the Executive Order

As we [previously wrote](#), on May 1 the White House issued an Executive Order on Securing the United States Bulk-Power System (“Executive Order”) that could result in restrictions on transactions involving non-U.S. bulk-power system electric equipment, potentially having significant impacts on utilities and the power and renewable industries.

If a transaction poses, e.g., an “unacceptable risk to the national security of the United States,” the Executive Order authorizes DOE to prohibit any “acquisition, importation, transfer, or installation” by a U.S. person or within the U.S., of any “bulk-power system electric equipment” with a certain nexus to a “foreign adversary.” A “transaction” can be “any acquisition, importation, transfer, or installation” of bulk-power system electric equipment that is “initiated” after May 1. However, the Executive Order was widely read as potentially causing problems where, for instance, equipment that was purchased prior to the May 1 date might subsequently be installed or transferred to another party – including through the sale of a project.

The initial press release caused a scramble amongst industry participants as to the scope of rules that might be implemented under the RFI, and in [an interview with Politico](#), U.S. Energy Secretary Dan Brouillette sought to allay developer fears, stating that he didn't expect "any problems or uncertainty" and indicated that the DOE would work with developers to address their concerns.

Nevertheless, while the DOE outreach helped to ease industry fears of a worst-case scenario where contracts deep into development or construction or operations are no longer economic, industry participants are struggling with three primary issues: (i) the decision over whether to proceed with current supply orders with equipment that might be impacted for new projects, (ii) increased diligence requirements from some lenders, and in certain cases additional mitigants in the form of reserves or audit or reporting requirements and (iii) continued unease over increased capital expenditures for existing projects without any means of recouping the costs (as affected utilities would be able to do by rate-basing any new equipment).

The comments are the power and renewable industry's opportunity to communicate their concern to DOE.

What we Know: Current Countries of Concern

Secretary Brouillette stated one concern is that a foreign adversary could provide faulty parts or equipment, or use its knowledge of cyber-system vulnerabilities "to carry out a targeted attack."

The RFI states that "the current list of 'foreign adversaries' consists of the governments" of China, Cuba, Iran, North Korea, Russia and Venezuela. This would appear to place an initial focus on state-owned companies, though under the Executive Order, it can extend to any party "owned or controlled by, or subject to the jurisdiction or direction of the foreign adversary." China and Russia are identified based on the Office of the Director of National Intelligence ("ODNI") National Counterintelligence and Security Center ("NCSC")'s assessment that they are "near-peer foreign adversaries" that "pose a major threat," e.g., to U.S. commercial and critical infrastructures.

ODNI also identified Iran and North Korea, both of which are subject to comprehensive U.S. economic sanctions. Cuba similarly is subject to comprehensive sanctions, as is the entire Maduro regime in Venezuela, over which the U.S. has sought to assert "[maximum pressure](#)." U.S. persons already are prohibited from doing business with sanctioned countries and sanctioned parties. However, their inclusion could be

relevant with respect to sub-tier suppliers, e.g., to the supply chains and U.S. contract considerations of companies in the European Union (EU) or in Asia, which currently generally do not impose comprehensive sanctions on countries like Cuba and Iran.

Information DOE Seeks

The Executive Order provides that DOE will “establish procedures to license transactions.” In doing so, first DOE is “soliciting views on safeguarding the supply chain from threats and vulnerabilities.” According to DOE, it seeks to prioritize the review of BPS electric equipment by function and impact to the overall BPS, and build upon government supply chain risk management (“SCRM”) and cybersecurity standards and best practices that already exist (e.g., the ODNI NCSC Supply Chain Directorate’s SCRM Best Practices, the NIST 800 series standards and NERC-CIP standards, and the Cybersecurity Capability Maturity Model (“C2M2”)).

DOE requests from industry stakeholders responses to several questions pertaining to what it has categorized into two categories: Supply Chain and Economic Analysis.

Supply Chain

The RFI asks several questions concerning how energy sector asset owners and vendors currently manage risk and exchange information, suggesting DOE is checking the viability of industry measures already in existence to safeguard BPS against risks, and whether further rules are needed.

Here, the focus is on certain transformers, reactive power equipment, circuit breakers and generation, including both the hardware and electronics associated with equipment monitoring, intelligent control and relay protection. The questions include:

- On a periodic basis, do energy sector asset owners and/or vendors conduct enterprise risk assessments, including a cyber maturity model evaluation?
- Do energy sector asset owners and/or vendors identify, evaluate and/or mitigate the risk of foreign ownership, control and influence (“FOCI”) with respect to foreign adversaries, including potential supply chain risks from sub-tier suppliers?
- Are incentives or changes to standards such as the NIST 800 series or SCRM standards necessary to maintain software integrity?

- What information is available concerning BPS electric equipment cyber vulnerability and what process does the energy sector have to share such information with utilities?
- What governance of sub-tier vendors do energy sector asset owners and/or vendors have in place, and is language for supply chain security included in procurement contracts and are metrics for supply chain security maintained?
- Can energy sector asset owners and/or vendors document their information sharing and testing programs that identify threats, vulnerabilities and indicators of compromise, and does the energy sector encourage information exchange with the federal government?
- What access control policies have been developed to monitor and restrict access during installation when a foreign adversary or associated persons installs BPS electric equipment at a BPS site in the U.S.?
- Are there critical mineral or supply chain materials used and what are they used for?

Economic Analysis

The RFI asks four questions pertaining to BPS electric equipment under the Executive Order, which suggests it wants to weigh the burden of additional compliance against the benefit of trying to protect U.S. industry and energy infrastructure from the threats it has identified:

- What are the estimated costs of developing, implementing and revising associated compliance plans and procedures?
- Are there categories of BPS electric equipment that are more reliant on vendors likely to become the subject of transaction reviews, and what are the related sourcing challenges and costs impacts for companies facing prohibited transactions for such equipment?
- Does the energy sector have a procedure to identify services, components and/or systems that are or should be covered by the Executive Order?
- What unique challenges could the Executive Order present to small businesses?

Comments can be filed via DOE's BPS portal, by email or by mail.

Key Takeaways

- Power grid companies should review their suppliers and their sub-tier suppliers to determine if any equipment or components are sourced from or travel through China, Cuba, Iran, North Korea, Russia or Venezuela.
- As part of the federal acquisition process, DOE is considering limited procurements, select build versus buy, the consequences of insufficient SCRM and evidence-based performance metrics that support a continuous improvement process.
- DOE appears to be considering establishing a regime of “transaction reviews,” which could be similar to that [proposed](#) by the U.S. Department of Commerce in connection with the [Information and Communications Technology and Services Supply Chain](#), conferring authority on the U.S. government potentially to reject, unwind or negotiate or impose mitigation measures on, specific transactions it finds of concern.
- Industry input could have an impact on the extent to which DOE in conjunction with other U.S. government agencies establishes specific criteria to devise a list of “pre-qualified” equipment and vendors, or identifies parties, countries, equipment or transactions that meet the Executive

[Read more insights from Kirkland's Energy & Infrastructure blog.](#)

Authors

[Mario Mancuso, P.C.](#)

Partner / [Washington, D.C.](#) / [New York](#)

[Sanjay José Mullick](#)

Partner / [Washington, D.C.](#)

[Brian C. Greene, P.C.](#)

Partner / [Washington, D.C.](#)

[Jeremy Iloulian](#)

Associate / [Washington, D.C.](#)

Related Services

Practices

- [Transactional](#)
- [Energy & Infrastructure](#)
- [International Trade & National Security](#)

This publication is distributed with the understanding that the author, publisher and distributor of this publication and/or any linked publication are not rendering legal, accounting, or other professional advice or opinions on specific facts or matters and, accordingly, assume no liability whatsoever in connection with its use. Pursuant to applicable rules of professional conduct, portions of this publication may constitute Attorney Advertising.

This publication may cite to published materials from third parties that have already been placed on the public record. The citation to such previously published material, including by use of "hyperlinks," is not, in any way, an endorsement or adoption of these third-party statements by Kirkland & Ellis LLP.