UNITED STATES OF AMERICA
BEFORE THE
DEPARTMENT OF ENERGY

Notice of Request for Information (RFI) on Ensuring the Continued Security of the United States Critical Electric Infrastructure	Docket No. 2021–08482

COMMENTS OF THE CALIFORNIA DEPARTMENT OF WATER RESOURCES STATE WATER PROJECT

The California Department of Water Resources ("CDWR") appreciates the opportunity to submit these comments in response to the Department of Energy's ("DOE") Notice of Request for Information (RFI) on Ensuring the Continued Security of the United States Critical Electric Infrastructure.[1]

CDWR provides a unique perspective on the issues addressed in the RFI. CDWR uses as much as 9.5 million megawatt-hours ("MWh") of electricity annually to achieve its primary mission of delivering water to approximately 27 million Californians. CDWR relies primarily on the bulk power system ("BPS") to meet its electricity needs, but it also owns and operates some of that BPS equipment. As both a BPS user that depends on others to provide high levels of electric reliability *and* a BPS owner responsible for providing that electric reliability, CDWR can offer a practical and balanced perspective on the issues.

[1] Notice of Request for Information (RFI) on Ensuring the Continued Security of the United States Critical Electric Infrastructure, 86 Fed. Reg. 21,309 (April 22, 2021) ("RFI").

CDWR supports DOE's approach of "addressing pervasive and ongoing grid security risks [through] a comprehensive long-term strategy."[2] These comments focus exclusively on the RFI's questions related to that long-term strategy. CDWR does not take a position on the advisability or feasibility of DOE issuing a prohibition order to address immediate threats.

I. DESCRIPTION OF CDWR

The California Department of Water Resources was established in 1956 by the California State Legislature with the mission to protect, conserve, develop, and manage California's water supply. CDWR operates the State Water Project, which supplies water to approximately 27 million Californians and 750,000 acres of farmland.

To fulfill its mission of supplying Californians with water, the State Water Project consumes 6 million to 9.5 million MWh of electricity annually. It supplies some of that energy itself, through its 5 hydroelectric power plants, and 4 pumping-generating plants. CDWR further manages its power operation through load management including demand response, purchase and sales transactions with other entities, and participation in the California Independent System Operator Corporation power markets.

DOE policies regulating the security of the power system will affect CDWR's power operations, both as an energy producer and an energy consumer, which are critical to the nation's most populous state and its largest economy.

II. COMMENTS

The following comments respond to Questions A.1, A.2, A.3 and A.4 of the RFI.

---

[2] RFI at 21,310.

A. DOE should establish a certification program for BPS equipment that will inform future utility procurement practices.

When procuring new BPS equipment and contracting with new vendors that provide services for BPS equipment, CDWR has developed a risk-informed, cost-conscious procurement program that complies with California law, adheres to all applicable Federal Energy Regulatory Commission ("FERC") and North American Electric Reliability Corporation ("NERC") requirements, and is informed by utility best practices. CDWR considers a wide range of security risks as part of its procurement process. Yet, despite its best-in-class procurement program, CDWR has limited ability to independently assess the risk of foreign ownership, control, or influence associated with BPS equipment and services that it procures. Even when the risk associated with a direct vendor is low, CDWR has little, if any, visibility into that vendor's supply chains, and thus CDWR cannot assess the risks associated with every subcomponent of BPS equipment that it purchases.

CDWR, like most owners of BPS equipment, depends on the federal government's intelligence capabilities to determine when particular countries or companies pose a risk to national security. Existing information sharing mechanisms—through the Department of Homeland Security's Cybersecurity and Infrastructure Security Agency, NERC, and industry trade associations—are helpful, but more can be done by the federal government to provide timely and meaningful information that could assist CDWR's (and others') procurement decisions. For example, the government could establish a mechanism to provide declassified information on companies that pose a national security risk or could provide security clearances to key BPS-owner personnel

for the purposes of sharing such information before it is declassified. These mechanisms should proceed pursuant to the confidentiality rules CDWR proposes in Section II.D.

CDWR believes that the best long-term strategy would be for DOE to develop a certification program that would identify vendors of BPS equipment and services that are not under the ownership, control, or influence of foreign adversaries and whose supply chains are similarly free from foreign influence. The federal government, not individual utilities or state agencies, is best placed to conduct that certification.[3]

CDWR urges DOE to develop such a certification program, which owners of BPS equipment can use to inform their future procurement practices, consistent with the following principles:

- **Collaborative**. While the federal government has intelligence expertise and capabilities, states have more expertise in local needs and policy objectives, and BPS owners have unique knowledge of their own systems. A certification program should involve input and collaboration from all relevant stakeholders.
- **Cost-conscious and risk-informed**. A certification program can have the unintended consequence of unduly narrowing the number of suppliers available to BPS owners, thereby unnecessarily increasing costs. The certification program should be well-designed to consider the risks posed by various types of equipment, and to not be overly restrictive unless justified by a risk assessment.

[3] We note that President Biden recently issued an Executive Order directing the National Institute of Standards and Technology to issue standards, procedures, or criteria regarding the security and integrity of the software supply chain procured by the Federal Government. Exec. Order No. 14,028, 86 Fed. Reg. 26,633 (May 17, 2021). Lessons from that initiative could inform how DOE could develop a certification program for vendors of BPS equipment.

- **Supportive of preferred vendors**. CDWR, like all California departments and many utilities around the country, supports small businesses, microbusinesses, and disabled veteran business enterprises. A certification program should allow for such businesses to easily obtain certification, especially when those businesses pose low risk of influence from foreign adversaries and their supply chains are made up of other certified vendors.
- **Auditable**. A vendor, once certified, must maintain that certification, and purchasers should be confident that certified vendors continue to be free from foreign influence. DOE should periodically audit certified vendors to ensure compliance.

B. DOE should develop a national risk-assessment framework to assist in identifying existing BPS equipment that contains components that pose a risk to national security.

Even if DOE were to develop a forward-looking certification to assist BPS owners with future procurement decisions, there remains the problem of identifying existing equipment that may pose national security risks and developing plans to mitigate those risks. BPS owners currently face challenges both with identification and with mitigation.

With regard to identification, BPS owners have limited information about which manufacturers are under the ownership, control, or influence of foreign adversaries. And even when the federal government has identified specific manufacturers—for example Huawei and ZTE—BPS owners cannot easily determine if their equipment includes components from those manufacturers.[4]

---

[4] *See* FERC/NERC, *Joint Staff White Paper on Supply Chain Vendor Identification* (Jul. 31, 2020),

Once equipment, or subcomponents, are identified, BPS owners must take appropriate action to mitigate that risk. Replacing the equipment, which might have many years of serviceable life remaining, may not be cost-effective or necessary. The appropriate mitigation actions will depend on the nature and use of the equipment, how it is interconnected with other equipment, the consequences of it being compromised, and other risk factors. For example, a protective relay that is not connected to the Internet (i.e., "air gapped") might be low risk, even if it contains components made by an identified foreign vendor. In contrast, an Internet-connected control system with unknown components may pose a greater risk.

CDWR believes that the best long-term strategy would be for DOE to establish a national risk-assessment framework to assist BPS owners in identifying threats and mitigating them. Such a risk assessment framework should be regularly updated to reflect the federal government's latest threat assessments and should be flexible enough that diverse BPS owners can use it to evaluate the specific risks to their equipment.

C. DOE should assist States and local governments with the financial burden of implementing these long-term strategies.

Purchasing new BPS equipment that is certified to be free of influence from foreign adversaries, and replacing existing BPS equipment that poses risks, will involve new, potentially significant, costs for BPS owners. "Public utilities," as defined in the Federal Power Act, are able to recover those increased costs through their rates regulated

---

https://www.nerc.com/pa/comp/CAOneStopShop/Joint%20Staff%20White%20Paper%20on%20Supply%20Chain_07312020.pdf (explaining the high probability that utilities unknowingly use networking and telecommunication equipment manufactured by Huawei or ZTE, because of "obscurely-labeled (or even unlabeled) components" that are included in equipment).

by FERC.[5] States and local governments, however, are not "public utilities" and are thus ineligible to recover increased costs through FERC-approved rates.[6]

If these long-term strategies, designed to protect national security, are implemented, entities like CDWR will be forced to pay increased rates to FERC-jurisdictional public utilities that implement these strategies and will incur the additional cost of implementing the same strategies itself. That double payment to support national security imposes a financial burden on state and local entities, and the DOE should provide assistance to mitigate that burden.

D. DOE should provide clear confidentiality rules.

Any long-term strategy DOE develops will apply in states with a variety of disclosure laws. As outlined above, DOE should continue to seek partnership with, and information from, utilities, Indian Tribes, and state and local entities to develop its long-term strategy. However, sourcing this information could create issues due to the variety of state-level disclosure requirements. DOE recently updated its own treatment of Critical Electric Infrastructure Information ("CEII") and Confidential Business Information and should use the standards adopted through that process to govern the provision of information provided in the course of the processes that come from this RFI.[7]

If entities provide CEII or Confidential Business Information as part of this collaborative process, it should be exempt from Freedom of Information Act requests and should not be provided even through a state disclosure request, consistent with 10 C.F.R.

---

[5] 16 U.S.C. § 824(e).

[6] 16 U.S.C. § 824(f).

[7] *See* Critical Electric Infrastructure Information; New Administrative Procedures, 83 Fed. Reg. 54,268 (October 29, 2018).

§ 1004.13(f). When determining whether provided information is CEII or Confidential Business Information pursuant to 10 C.F.R. § 1004.13(g)(6), information provided in this proceeding that is marked as CEII or Confidential Business Information should be given a rebuttable presumption that it is CEII or Confidential Business Information.

A clear confidentiality standard and a presumption of confidentiality will encourage transparency in the public-private partnership needed to develop a long-term strategy that will protect the grid from foreign threats.

III. CONCLUSION

A long-term strategy to address the threats of foreign ownership and control of equipment used for the BPS is essential to ongoing grid security. State, local and tribal owners and users of the BPS face distinct challenges compared to large, investor-owned utilities. CDWR urges the DOE to work in partnership, particularly with states, to develop long-term programs that will cost-effectively mitigate risks of existing BPS equipment that may pose threats and that will ensure future procurement of BPS equipment is informed by the best available intelligence of foreign threats.

Respectfully submitted,

/s/ *Katharine S. Killeen*

Katharine S. Killeen,
Assistant Chief Counsel
California Department of Water Resources
P.O. Box 899
Sacramento, CA 94236-0001
Katharine.Killeen@water.ca.gov

June 7, 2021