UNITED STATES OF AMERICA
BEFORE THE
DEPARTMENT OF ENERGY

Notice of Request for Information on Ensuring the Continued Security of the United States Critical Electric Infrastructure	)))	DOE_FRDOC_0001-4185

COMMENTS OF THE ISO/RTO COUNCIL

The ISO/RTO Council ("IRC")[1] submits these comments and responses in reply to the United States Department of Energy's ("DOE") Notice of Request for Information on Ensuring the Continued Security of the United States Critical Electric Infrastructure published in the Federal Register on April 22, 2021.[2] In the RFI, the DOE seeks information on various aspects of the electric infrastructure as the DOE develops a strengthened approach to address the supply chain security of the electricity subsector in the United States.

I. ANSWERS TO QUESTIONS POSED IN THE REQUEST FOR INFORMATION

The IRC provides the following responses to questions posed by the DOE in the RFI.[3]

---

[1] The IRC comprises the following independent system operators ("ISOs") and regional transmission organization ("RTOs"): Alberta Electric System Operator ("AESO"), California Independent System Operator ("CAISO"), Electric Reliability Council of Texas, Inc. ("ERCOT"), the Independent Electricity System Operator of Ontario, Inc. ("IESO"), ISO New England Inc. ("ISO-NE"), Midcontinent Independent System Operator, Inc. ("MISO"), New York Independent System Operator, Inc. ("NYISO"), PJM Interconnection, L.L.C. ("PJM"), and Southwest Power Pool, Inc. ("SPP"). The AESO is not subject to the DOE's jurisdiction with respect to the matters addressed in this rulemaking, however, joins these comments. The IESO is not subject to the DOE's jurisdiction with respect to the matters addressed in this rulemaking and, therefore, does not join these comments.

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

[3] As permitted in the RFI, the IRC responds to only certain questions posed. *See* RFI at 21,310 ("Respondents are not required to address all questions.").

A. *Response to Question in Section II.A.2: What specific additional actions could be taken by regulators to address the security of critical electric infrastructure and the incorporation of criteria for evaluating foreign ownership, control, and influence into supply chain risk management, and how can the Department of Energy best inform those actions?*

Regulatory actions to address supply chain to date have focused on managing risks in the deployment processes, installation of software, and management of vendor remote access. The North American Electric Reliability Corporation ("NERC") Reliability Standards on supply chain management largely focus on ensuring that each regulated entity develop its own supply chain management plan. Although this was an appropriate starting place, reducing supply chain risks also requires direction and information on specific supply chain threats that only the Federal government can provide due to the classified nature of such information.

The use of targeted Prohibition Orders could complement the bottom-up approach of the NERC Reliability Standards. However, the Prohibition Orders issued to date have focused on service to particular end-users such as infrastructure serving defense critical facilities. Given the interconnected nature of the transmission grid, future Prohibition Orders should utilize a risk-based approach for sources of equipment that can impact grid operations as a whole rather than target service to particular end-use segments.

Innovative technological approaches are also necessary to strengthen the protection of the supply chain. The Presidential Executive Order on cybersecurity issued on May 12, 2021 recommends security best practices, the use of zero trust architecture, the adoption of cloud services, and advanced data analytics to reduce cybersecurity risks; however, existing regulatory standards may not permit the adoption of new technological approaches. Therefore, future regulatory action should ensure that regulatory standards will support or permit additional innovative technology and future developments of network architecture to better protect information technology systems.

B. Responses to Questions in Section II.A.3: What actions can the Department take to facilitate responsible and effective procurement practices by the private sector? What are the potential costs and benefits of those actions?

The DOE should consider approaches that require suppliers of certain products and services to the electric industry to provide more transparency and clarity for entities that use those products or services for, or in support of, critical electric system infrastructure. Reducing supply chain risks requires information about suppliers that only the Federal government can provide. Providing mechanisms for greater transparency and security of that information will be important. Certain information and directives provided to the private sector by the Federal government have created some transparency. For example, the Federal government has provided the private sector with the specific names of corporations that cannot be used as suppliers. Other information provided to the private sector broadly extends to nation-states, leaving entities without sufficient information to vet suppliers that may pose a risk to the nation.

In addition to increased transparency, any future information or directives provided by the Federal government to protect the supply chain of the electricity sector should not focus on specific end-use sectors given the interconnected nature of the transmission grid and the inability to segment operations for a particular end-use sector. Future action by the DOE should consider how to include other critical infrastructure sectors upon which the electricity industry relies because of the interdependence of these sectors (e.g., natural gas sector, telecommunications sector, and fuel oil pipelines).

C. Response to Question in Section II.A.4: Are there particular criteria the Department could issue to inform utility procurement policies, state requirements, or FERC mandatory reliability standards to mitigate foreign ownership, control, and influence risks?

Currently, electric entities subject to mandatory NERC Reliability Standards analyze security-risk issues and questions in the procurement process based on their own understanding of suppliers, supply chains, and security risks. As stated above, more specific information and guidance on potential threats from the Federal government on how to make informed, risk-based decisions for critical infrastructure procurement would increase the ability to successfully identify security risks in the procurement process.

D. Response to Question in Section II.B.1: To ensure the national security, should the Secretary seek to issue a Prohibition Order or other action that applies to equipment installed on parts of the electric distribution system, i.e., distribution equipment and facilities?

The IRC recommends that the electric distribution system should be included in any such Prohibition Orders or other related actions. Isolated cybersecurity incidents and attacks on the electric distribution system may result in little or no impact on the rest of the electric power system, but a large-scale cybersecurity incident on the electric distribution system could disrupt a significant amount of load. This, in turn, could negatively affect the ability of system operators to maintain system balance and frequency or disrupt communications.

Moreover, the increased interconnection of distributed generation to the electric distribution system increases the risk that a cyberattack on the electric distribution system could also disrupt generation. In other words, with increased distributed generation, cyberattacks on the electric distribution system could disrupt, not just load, but also generation, which is also required to maintain the generation-to-load balance that is critical to the stability of the interconnected electric power system. For these reasons, the IRC suggests that DOE's actions in this area should also encompass a targeted risk-based analysis of threats from foreign attachments to the electric distribution system.

The IRC recognizes the importance of Prohibition Orders, especially for short-term actions to support national security. In the longer term, Prohibition Orders are difficult to maintain, and place administrative burdens that do not provide commensurate security value. As a result, the DOE should consider more efficient methods that accomplish similar benefits to Prohibition Orders while providing more transparency and reducing administrative burden. For example, the DOE should consider how to utilize an open certification program to clear vendors that may be selected to support the distribution and transmission systems. The DOE should also consider the development of a trusted vendor list to support consistent, risk-based decision-making in the procurement process. Finally, DOE should consider guidance to asset owners on targeted mitigation measures that could be used in the event that "prohibited" vendor products have already been used within critical infrastructure.

E. Response to Question in Section II.B.2: In addition to DCEI, should the Secretary seek to issue a Prohibition Order or other action that covers electric infrastructure serving other critical infrastructure sectors including communications, emergency services, healthcare and public health, information technology, and transportation systems?

As noted above, given the interconnected nature of the grid, the DOE should not issue Prohibition Orders targeted to particular end-use sectors. Rather, any Prohibition Orders should provide specific information about companies, nation states, and particular equipment types that present risks to the supply chain of critical equipment.

The IRC also urges the DOE to clarify that Prohibition Orders and other actions resulting from this initiative will also apply to critical infrastructure beyond the electric infrastructure to the extent such infrastructure is required to ensure reliable electric service, an input to the provision of electricity, and within the scope of the DOE's efforts. The DOE's question focuses on "a Prohibition Order or other action that covers electric infrastructure serving other critical infrastructure." However, the focus on electric infrastructure ignores the fact that a number of sectors (including the natural gas sector, information technology sector, telecommunications sectors and fuel oil pipelines) provide critical inputs in the way of fuel or infrastructure that are needed to "keep the lights on." To mitigate cyber security risks to the reliable operation of the electricity system, any Prohibition Orders or actions should also apply to critical infrastructure on which the electricity sector relies.

F. *Response to Question in Section II.B.3: In addition to critical infrastructure, should the Secretary seek to issue a Prohibition Order or other action that covers electric infrastructure enabling the national critical functions?*

See the IRC answer to the question in Section II.B.2 of the RFI above.

G. *Response to Question in Section II.B.4: Are utilities sufficiently able to identify critical infrastructure within their service territory that would enable compliance with such requirements?*

The electric system is complicated and interdependent. It will be challenging to single out a certain portion of the system as containing critical infrastructure. As a result, any Prohibition Order or other action should include all entities involved in the system and avoid singling out specific end-use sectors.

II. CONCLUSION

The IRC stands ready to work with the DOE on this important effort. We look forward to continuing dialogue and work with DOE on this important task.

Respectfully submitted,

/s/ Tyler E. Barnett
Maria Gulluni
Vice President & General Counsel

Tyler E. Barnett
Corporate Counsel

ISO New England Inc.
One Sullivan Road
Holyoke, Massachusetts 01040
tbarnett@iso-ne.com

/s/ James Burlew
Craig Glazer
Vice President-Federal Government Policy

James M. Burlew
Senior Counsel

PJM Interconnection, L.L.C.
2750 Monroe Boulevard
Audubon, Pennsylvania 19403
james.burlew@pjm.com

/s/ Andrew Ulmer
Roger E. Collanton
General Counsel

Anthony Ivancovich
Deputy General Counsel, Regulatory

Andrew Ulmer Director
Federal Regulatory Affairs

California Independent System Operator Corporation
250 Outcropping Way
Folsom, California 95630
amckenna@caiso.com

/s/ Christopher R. Sharp
Robert E. Fernandez
General Counsel

Raymond Stalter
Director of Regulatory Affairs

Carl F. Patka
Assistant General Counsel

Christopher R. Sharp
Senior Compliance Attorney

New York Independent System Operator, Inc.
10 Krey Boulevard
Rensselaer, NY 12144
cpatka@nyiso.com

<u>/s/ Andre T. Porter</u>
Andre T. Porter
Vice President, General Counsel & Secretary

Mary-James Young
Senior Corporate Counsel

Midcontinent Independent System Operator, Inc.
720 City Center Drive
Carmel, Indiana 46032
aporter@misoenergy.org

<u>/s/ Paul Suskie</u>
Paul Suskie
Executive Vice President & General Counsel

Mike Riley
Associate General Counsel

Southwest Power Pool, Inc.
201 Worthen Drive
Little Rock, Arkansas 72223-4936
psuskie@spp.org

<u>/s/ Diana Wilson</u>
Diana Wilson
Director Enterprise Risk Management and Compliance

Alberta Electric System Operator
#2500, 330 — 5 Avenue SW
Calgary, Alberta T2P 0L4
Diana.wilson@aeso.ca

<u>/s/ Chad V. Seely</u>
Chad V. Seely
Vice President and General Counsel

Nathan Bigbee
Assistant General Counsel

Brandon Gleason
Senior Corporate Counsel

Electric Reliability Council of Texas, Inc.
7620 Metro Center Drive
Austin, Texas 78744
chad.seely@ercot.com

June 7, 2021