

February 6, 2017

VIA E-MAIL

Mr. Jeffrey Baumgartner
U.S. Department of Energy
Office of Electricity Delivery and Energy Reliability
Mail Stop OE-20, Room 8G-017
1000 Independence Ave., SW
Washington, DC 20585

**Re: ISO-RTO Council Comments on Notice of Proposed Rulemaking Regarding
Grid Security Emergency Orders: Procedures for Issuance–RIN 1901–AB40**

Dear Mr. Baumgartner:

Pursuant to the notice of proposed rulemaking the U.S. Department of Energy (“DOE”) published in the Federal Register on December 7, 2016 (“NOPR”), the ISO-RTO Council (“IRC”)¹ hereby submits comments in response to the request for comments contained in the NOPR. The proposed procedures, if adopted, are intended to ensure the expeditious issuance of emergency orders under the Federal Power Act.

IRC COMMENTS

The DOE NOPR is a helpful first step in setting forth procedures on how the Secretary of Energy (“Secretary”) will administer his new authority provided pursuant to the *Fixing America’s Surface Transportation Act* (“FAST Act”), 16 U.S.C. 824 *et seq.* Although any rulemaking must balance the need for flexibility versus the need for clarity, the IRC believes there are several sections in the NOPR in which additional clarity is needed to prevent confusion, miscommunication, or procedures that could be abused. The IRC’s specific recommendations in this regard are set forth below.

1. The Proposed Process for Issuing an Emergency Order

The authority of the Secretary under the FAST Act is extremely broad. It is critical that this sweeping authority be used prudently and surgically. For example, as cyberattack attempts occur virtually every day on isolated pieces of utility equipment, it would not be appropriate for the Secretary to issue emergency orders for isolated actions affecting a single utility with no indication that the attack is indicative of a larger threat to the bulk electric system. As a result,

¹ The IRC comprises the 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”). As Canadian entities, AESO and IESO are not subject to the DOE’s jurisdiction with respect to the matters addressed in this rulemaking and, therefore, do not join these Comments.

flexible but defined standards are needed to govern the exercise of the Secretary's new vast authority under the FAST Act. To ensure that there are some standards around the Secretary's consideration of use of this authority while still ensuring flexibility in application of that authority, the IRC recommends the following:

- a. *Vetting of Emergency Orders with the ESCC*—The industry and the DOE have worked together to create the Electric Sector Coordinating Council (“ESCC”) to serve as the vehicle for communication and coordination between the DOE and the industry both for physical and cybersecurity. The ESCC consists of representatives of all industry segments including the generator sector, the RTOs and ISOs, public power, and even Canadian entities. The IRC recommends that the Final Rule maintain the commitment that, to the extent practicable, requests for an order from the Secretary under his FAST Act authority be first vetted with the ESCC and that requests for modifications to orders be similarly vetted. The ESCC has proven itself both nimble and able to come together on very short notice. To avoid a multitude of “one-off” requests for emergency orders even for minor malware instances, a process for prompt vetting of such decisions with the ESCC should be explicitly written into the Final Rule as a key condition precedent to the issuance of an emergency order; and
- b. *Providing Clarification in the Final Rule of a Flexible but Implementable Standard to Govern the Exercise of the Secretary's Authority*—As noted above, the sweeping authority of the FAST Act should be reserved for true widespread grid security emergencies.² By supplementing the Secretary's existing authority under Section 202 of the Federal Power Act, Congress clearly was trying to address broader cyber and physical grid security threats than those more localized events which could be addressed through existing authority. However, the recent event in Burlington, Vermont underscores the danger that isolated incidents at a utility (and in the case of Burlington not affecting the grid itself) can quickly create the perception that sweeping actions—including remedial orders such as those contemplated under the NOPR—may be appropriate when in fact they are neither necessary nor prudent. On the other hand, the IRC recognizes the difficulty of listing in the Final Rule, with specificity, the kinds of events that could trigger utilization of the Secretary's authority under the FAST Act. Accordingly, the IRC proposes that the Final Rule contain a specific standard, albeit a flexible one, to govern the Secretary's consideration of a request for declaring a grid security emergency. The IRC would propose that the Final Rule set forth a threshold standard by indicating that such an order would be based on a finding of:

“imminent widespread threat to the security of the grid which cannot be ameliorated by the action of a single entity.”

² It is worth noting that nothing in the FAST Act authority impacts the President's or the Secretary's authority to address more local events. Specifically, the Secretary continues to retain authority for more targeted orders affecting particular utilities or localities through his existing Section 202(c) authority, and the President retains his existing authority to address local emergencies under the Stafford Act.

In adopting this proposed standard, the Final Rule could make clear that the Secretary would retain significant discretion in applying that standard based on the facts presented. Nevertheless, such a threshold standard governing action by the Secretary would avoid individual entities simply seeking “one-off” requests motivated more by attempts to avoid later potential regulatory disallowances in lieu of a determination that the threat is more widespread.

2. *Meaning of the Term “Electric Reliability Entity”*

The NOPR refers to ‘electric reliability entity’ but does not define the term. The IRC believes that in almost all cases, the NERC Reliability Coordinators (“RCs”) are the appropriate entities to receive such orders. As a result, the IRC recommends that in order to avoid confusion in real time as to who is the “electric reliability entity,” the term be defined in the Final Rule as “the entity registered with the North American Reliability Corporation as the Reliability Coordinator for the affected part of the bulk power system.” Those entities are listed at <http://www.nerc.org/pa/rrm/TLR/Pages/Reliability-Coordination.aspx>. Moreover, the DOE should clarify in its procedures that it will consult with the affected RCs before issuing a directive that impacts a system under an RC’s control. The central role taken by an RC puts it in a position of needing to be aware of nearly any corrective measure that might be ordered in its area following a physical attack, cyber-attack, or geomagnetic disturbance event. Because RCs already have general reliability responsibility for their control areas, RCs will likely already be taking necessary measures to address the reliability impact. Ordering additional measures could exacerbate reliability problems, so consultation is critical.

3. *The Process to Request an Emergency Order Following a Grid Security Emergency Declaration*

Although not currently contemplated in the NOPR, the DOE should consider a process that provides a clear and expedited process specifying how entities may request a DOE emergency order, following a Presidential declaration of a grid security emergency (that order being subject to the vetting through the ESCC as noted above). The process should describe how an affected party may actually submit such a request and what supporting information is needed to be provided to ensure that consideration by the Secretary is based on documented facts (rather than rumor and anecdote) to the extent these facts and investigation results are available in real time. The process should specify the communication mechanisms which should include written communications vetted with the ESCC and also provide a means for back-up communication channels should a cyber or physical attack disable one or more normal communication channels for effectuating such a request.

4. *Process for Communicating Emergency Orders*

The NOPR provides no detail about the nature of the communication of temporary emergency measures. Notice of the specific method of communication is essential to enable affected parties to authenticate the orders and to adequately prepare to receive and act on orders

expeditiously. Entities receiving such orders will need to be able to immediately determine that a communication has come from the DOE and not from someone falsely purporting to be DOE. Orders communicated through traditional telephone or email communications may not provide sufficient authentication.

5. *Interagency Coordination*

The IRC suggests that as an accompaniment to the Final Rule, the DOE should coordinate through a memorandum of understanding or other means (and communicate to the industry) additional clarity concerning the interagency coordination to be undertaken under these provisions of the FAST Act and their relationship to existing interagency coordination directives to avoid confusion and delay. For example, Presidential Policy Directive 41 titled *United States Cyber Incident Coordination* clarifies and codifies lines of responsibility as they apply to “significant cyber incidents. Under the directive, the Department of Homeland Security (“DHS”) is the lead entity on asset protection with the Office of the Director of National Intelligence taking the lead on intelligence support activities. However, under the DOE NOPR, the DOE undertakes the coordination of protection and restoration of critical electric infrastructure and defense of the same during an emergency. Without well planned interagency coordination procedures and clarity in the Final Rule as to how these various directives and responsibilities are to be effectuated by the various federal agencies, there could be an overlap in authority between the DHS, the Director of National Intelligence, and the DOE as they all scramble to take action to protect critical infrastructure.

Similarly, under the *Robert T. Stafford Disaster Relief and Emergency Assistance Act*, 42 U.S.C. 5121 *et seq.*, there are two types of Presidential declarations: emergency declarations and disaster declarations. The first is focused on removing obstacles to providing federal assets to support a disaster response and enabling the Federal Emergency Management Agency to preside as the lead federal agency for coordinating resources. The second is designed for activating federal support for utilities including municipally-owned electric utilities and electric cooperatives. While the NOPR correctly focuses on grid-only events, it is unclear how interagency coordination will occur for an event that is classified as two or more types of emergencies (*e.g.*, an event that classifies as a grid security emergency, emergency declaration, and a disaster declaration). Clarification should be provided in the Final Rule as to the relationship of the Secretary’s implementation of its FAST Act authority and the Secretary’s coordination with other federal agencies under this authority with the existing interagency coordination protocols that specify the key role of the DHS and the Director of National Intelligence.

6. *Requests for Clarification or Reconsideration of a DOE Emergency Order*

Under the NOPR, anyone subject to an order may seek clarification or reconsideration from DOE which request the DOE may grant or deny (including abrogation or modification of the final emergency order) with or without further proceedings. The IRC remains concerned that this completely open-ended process could lead to a flood of “one off” requests by individual entities that could be acted upon by the Secretary without the appropriate vetting or notification.

The IRC recognizes the need for speed in such instances but, in order to avoid a plethora of “one-off” requests, proposes that any such requests would be vetted with the ESCC prior to the Secretary taking action. Moreover, any such modification of an order (and the order itself) should be communicated *in writing* to all affected parties with the basis for the modification explained and clarity provided as to the scope and extent of the modified order. Although telephonic communication and explanation of the Secretary’s actions is most appropriate, the actual order itself (and any modifications thereto) should be in writing and accessible to affected parties to avoid the potential for miscommunication that can occur through oral communications. In order to carry out these suggestions, the IRC suggests that a pre-defined, expedited appeal process be spelled out in the Final Rule.

The IRC appreciates the opportunity to provide these comments to the DOE and urges that the specific recommendations set forth herein be adopted in the Final Rule. The IRC members are prepared to provide any information or assistance the DOE may need in developing this Final Rule and in addressing specific incidents through consultation with the ESCC.

Respectfully submitted,

/s/ Theodore J. Paradise

Raymond W. Hepper
Vice President, General Counsel, and Secretary
Theodore J. Paradise
Assistant General Counsel, Operations and
Planning
ISO New England Inc.
One Sullivan Road
Holyoke, Massachusetts 01040
tparadise@iso-ne.com

/s/ Anna McKenna

Roger E. Collanton, General Counsel
Anna McKenna
Assistant General Counsel, Regulatory
Andrew Ulmer Director, Federal Regulatory
Affairs
**California Independent System Operator
Corporation**
250 Outcropping Way
Folsom, California 95630
amckenna@caiso.com

/s/ James M. 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/ Christopher Sharp

Robert E. Fernandez, General Counsel
Raymond Stalter
Director of Regulatory Affairs
Christopher Sharp
Compliance Attorney
**New York Independent System Operator,
Inc.**
10 Krey Boulevard
Rensselaer, NY 12144
skeegan@nyiso.com

/s/ Stephen G. Kozey

Stephen G. Kozey
Senior Vice President
Joseph G. Gardner
Vice President & Chief Compliance Officer
**Midcontinent Independent System
Operator, Inc.**
720 City Center Drive
Carmel, Indiana 46032
stevekozey@misoenergy.org

/s/ Nathan Bigbee

Chad V. Seely
Vice President & General Counsel
Nathan Bigbee
Assistant General Counsel
Electric Reliability Council of Texas, Inc.
7620 Metro Center Drive
Austin, Texas 78744
nathan.bigbee@ercot.com

/s/ Paul Suskie

Paul Suskie
Executive Vice President & General Counsel
Tessie Kentner
Senior Attorney
Southwest Power Pool, Inc.
201 Worthen Drive
Little Rock, Arkansas 72223-4936
psuskie@spp.org