

146 FERC ¶ 61,166
UNITED STATES OF AMERICA
FEDERAL ENERGY REGULATORY COMMISSION

Before Commissioners: Cheryl A. LaFleur, Acting Chairman;
Philip D. Moeller, John R. Norris,
and Tony Clark.

Reliability Standards for
Physical Security Measures

Docket No. RD14-6-000

ORDER DIRECTING FILING OF STANDARDS

(Issued March 7, 2014)

1. As part of its ongoing oversight of the Bulk-Power System, and pursuant to section 215(d)(5) of the Federal Power Act (FPA), the Commission directs the North American Electric Reliability Corporation (NERC), as the Commission-certified Electric Reliability Organization (ERO), to submit for approval one or more Reliability Standards that will require certain registered entities to take steps or demonstrate that they have taken steps to address physical security risks and vulnerabilities related to the reliable operation of the Bulk-Power System. The proposed Reliability Standards should require owners or operators of the Bulk-Power System, as appropriate, to identify facilities on the Bulk-Power System that are critical to the reliable operation of the Bulk-Power System. Then, owners or operators of those identified critical facilities should develop, validate and implement plans to protect against physical attacks that may compromise the operability or recovery of such facilities. The Commission directs NERC to submit the proposed Reliability Standards to the Commission within 90 days of the date of this order.

2. The Commission appreciates that many owners and operators of critical facilities already have separately taken steps to enhance the physical security of their facilities. We also recognize that there is not a “one size fits all” response to protect against physical security threats, and we do not seek to impose one by this order. However, this action will better ensure the reliable operation of the Bulk-Power System.

I. Background

3. Section 215 of the FPA requires the Commission to certify an ERO to develop mandatory and enforceable Reliability Standards, subject to Commission review and

approval.¹ Once approved, the Reliability Standards may be enforced in the United States by the ERO, subject to Commission oversight, or by the Commission independently.

4. Pursuant to section 215(d)(5) of the FPA, the Commission has the authority, upon its own motion or upon complaint, to order the ERO to submit to the Commission a proposed Reliability Standard or a modification to a Reliability Standard that addresses a specific matter if the Commission considers such a new or modified Reliability Standard appropriate to carry out section 215 of the FPA.²

II. Discussion

5. Physical attacks to the Bulk-Power System can adversely impact the reliable operation of the Bulk-Power System, resulting in instability, uncontrolled separation, or cascading failures. However, the current Reliability Standards do not specifically require entities to take steps to reasonably protect against physical security attacks on the Bulk-Power System.³ Therefore, to carry out section 215 of the FPA and to provide for the reliable operation of the Bulk-Power System, the Commission directs the ERO to develop and file for approval proposed Reliability Standards that address threats and vulnerabilities to the physical security of critical facilities on the Bulk-Power System. Such Reliability Standards will enhance the Commission's ability to assure the public that critical facilities are reasonably protected against physical attacks.

6. The Reliability Standards should require owners or operators of the Bulk-Power System to take at least three steps to address the risks that physical security attacks pose

¹ 16 U.S.C. § 824o (2012).

² 16 U.S.C. § 824o(d)(5); 18 C.F.R. § 39.6(f) (2013).

³ The current Reliability Standards use the words “physical” and “cyber” to describe two methods of attacking utility assets. For example, Reliability Standard CIP-006-3c requires a physical security program for the protection of “Critical Cyber Assets,” but does not address facilities that are not so categorized. Similarly, Reliability Standard EOP-004-2 requires only that entities report, among other things, physical damage to, destruction of, and physical threats to, a facility due to intentional harm or suspicious activity. *See* Reliability Standard EOP-004-2, Event Reporting, Attachment 1.

to the reliable operation of the Bulk-Power System.⁴ First, the Reliability Standards should require owners or operators of the Bulk-Power System to perform a risk assessment of their systems to identify their “critical facilities.” A critical facility is one that, if rendered inoperable or damaged, could have a critical impact on the operation of the interconnection through instability, uncontrolled separation or cascading failures on the Bulk-Power System.⁵ Methodologies to determine these facilities should be based on objective analysis, technical expertise, and experienced judgment. The Commission is not requiring NERC to adopt a specific type of risk assessment, nor is the Commission requiring that a mandatory number of facilities be identified as critical facilities under the Reliability Standards.⁶ Instead, the Commission is directing NERC to develop Reliability Standards that will ensure that owners or operators of the Bulk-Power System identify those facilities that are critical to the reliable operation of the Bulk-Power System such that if those facilities are rendered inoperable or damaged, instability, uncontrolled separation or cascading failures could result on the Bulk-Power System and thereby warrant the directive imposed here.

7. Issuance of this directive will help provide for the resiliency and reliable operation of the Bulk-Power System. To that end, the proposed Reliability Standards should allow owners or operators to consider resilience of the grid in the risk assessment when identifying critical facilities, and the elements that make up those facilities, such as transformers that typically require significant time to repair or replace. As part of this process, owners or operators may consider elements of resiliency such as how the system

⁴ Some of the requirements imposed by these newly proposed Reliability Standards may best be performed by the owner and other activity may best be performed by the operator. In the proposed Reliability Standards, NERC should clearly indicate where the owner is the entity responsible for complying with each requirement, and where the operator is responsible for compliance. Further, in its filing, NERC should justify its selection of owner or operator for the proposed requirements.

⁵ We recognize that owners and operators may also take steps to protect facilities necessary to serve critical load on their systems, even if the inoperability or damage to those facilities would not result in instability, uncontrolled separation or cascading failures on the Bulk-Power System. However, the Reliability Standards that we are ordering today apply only to critical facilities that, if rendered inoperable or damaged, could have a critical impact on the operation of the interconnection through instability, uncontrolled separation or cascading failures on the Bulk-Power System.

⁶ However, the Commission expects that critical facilities generally will include, but not be limited to, critical substations and critical control centers.

is designed, operated, and maintained, and the sophistication of recovery plans and inventory management.⁷

8. In the second step, the Reliability Standards should require owners or operators of the identified critical facilities to evaluate the potential threats and vulnerabilities to those identified facilities. The threats and vulnerabilities may vary from facility to facility based on factors such as the facility's location, size, function, existing protections and attractiveness as a target. Thus, the Reliability Standards should require the owners or operators to tailor their evaluation to the unique characteristics of the identified critical facilities and the type of attacks that can be realistically contemplated. NERC should also consider in the standards development process requiring owners and operators to consult with entities with appropriate expertise as part of this evaluation process.

9. Third and finally, the Reliability Standards should require those owners or operators of critical facilities to develop and implement a security plan designed to protect against attacks to those identified critical facilities based on the assessment of the potential threats and vulnerabilities to their physical security. The Reliability Standards themselves need not dictate specific steps an entity must take to protect against attacks on the identified facilities. However, the Reliability Standards need to require that owners or operators of identified critical facilities have a plan that results in an adequate level of protection against the potential physical threats and vulnerabilities they face at the identified critical facilities.

10. All three steps of compliance with the Reliability Standard described above could contain sensitive or confidential information that, if released to the public, could jeopardize the reliable operation of the Bulk-Power System. Guarding sensitive or confidential information is essential to protecting the public by discouraging attacks on critical infrastructure. Therefore, NERC should include in the Reliability Standards a procedure that will ensure confidential treatment of sensitive or confidential information but still allow for the Commission, NERC and the Regional Entities to review and inspect any information that is needed to ensure compliance with the Reliability Standards.

11. In addition, the risk assessment used by an owner or operator to identify critical facilities should be verified by an entity other than the owner or operator. Such verification could be performed by NERC, the relevant Regional Entity, a Reliability Coordinator, or another entity. The Reliability Standards should include a procedure for the verifying entity, as well as the Commission, to add or remove facilities from an owner's or operator's list of critical facilities. Similarly, the determination of threats and

⁷ See NERC's report on Severe Impact Resilience at http://www.nerc.com/comm/OC/SIRTF%20Related%20Files%20DL/SIRTF_Final_May_9_2012-Board_Accepted.pdf.

vulnerabilities and the security plan should also be reviewed by NERC, the relevant Regional Entity, the Reliability Coordinator, or another entity with appropriate expertise. Finally, the Reliability Standards should require that the identification of the critical facilities, the assessment of the potential risks and vulnerabilities, and the security plans be periodically reevaluated and revised to ensure their continued effectiveness. NERC should establish a timeline for when such reevaluations should occur.

12. Under the Reliability Standards, we anticipate that the number of facilities identified as critical will be relatively small compared to the number of facilities that comprise the Bulk-Power System. For example, of the many substations on the Bulk-Power System, our preliminary view is that most of these would not be “critical” as the term is used in this order. We do not expect that every owner and operator of the Bulk-Power System will have critical facilities under the Reliability Standard. We also recognize that the industry has engaged in longstanding efforts to address the physical security of its critical facilities. Thus, NERC should develop an implementation plan that requires owners or operators of the Bulk-Power System to implement the Reliability Standards in a timely fashion, balancing the importance of protecting the Bulk-Power System from harm while giving the owners or operators adequate time to meaningfully implement the requirements. NERC should file the plan with the Reliability Standards for Commission review.⁸

13. In directing NERC to submit these proposed Reliability Standards, we are not proposing specific requirements or otherwise pre-judging what NERC may submit. Instead, in this order we identify concerns that should be addressed in the NERC standards development process. NERC may develop Reliability Standards that address these concerns in an equally efficient and effective manner. However, we expect NERC to support its proposed Reliability Standards and explain how they address the Commission’s concerns. The Commission will consider the Reliability Standards that NERC submits for approval in a rulemaking docket, which will include an opportunity for comment.

The Commission orders:

(A) NERC is hereby directed to file proposed Reliability Standards within 90 days of the date of this order, as discussed in the body of this order.

⁸ The implementation plan should include timeframes for completion of the risk assessment, threat and vulnerability assessments, and development and implementation of the security plan. NERC should include adequate detail in the implementation plan to inform the Commission of the implementation of the Reliability Standards, but in a way that does not disclose information that may be sensitive or confidential.

(B) Any interested person desiring to be heard in this proceeding should file a notice of intervention or motion to intervene with the Federal Energy Regulatory Commission, 888 First Street, N.E., Washington, DC 20426, in accordance with Rule 214 of the Commission's Rules of Practice and Procedure (18 C.F.R. § 385.214), within 21 days of the date of this order.

By the Commission. Commissioner Norris is concurring with a separate statement attached.

(S E A L)

Kimberly D. Bose,
Secretary.

UNITED STATES OF AMERICA
FEDERAL ENERGY REGULATORY COMMISSION

Reliability Standards for
Physical Security Measures

Docket No. RD14-6-000

(Issued March 7, 2014)

NORRIS, Commissioner, *concurring*:

I support this order because I believe it is appropriate for the Commission, NERC and our nation's electricity sector to work together to establish a standard addressing physical vulnerabilities with respect to our nation's power grid. We have made significant progress on electric grid reliability in recent years, largely due to the efforts of NERC and stakeholders. Such progress includes a number of steps taken by the Commission, NERC, and industry to bolster our electric grid security against physical vulnerabilities. I support directing NERC to draft rules that enhance the reliability of the grid by further protecting it against physical vulnerabilities. While I am generally supportive of the approach set forth in the order, I do have several concerns that I feel compelled to address.

First, I have concerns regarding the procedural mechanism that the Commission is utilizing in this order. Upon the issuance of today's order, NERC will be expected to institute a standards development process, resulting in the submission of a reliability standard within 90 days. The Commission will be unable to communicate with interested parties after today regarding that standard development process for an as of yet undetermined period of time because of the Commission's *ex parte* rules.

I believe that the standards development process could be weakened by this lack of engagement between the Commission and industry during that process. The owners and operators of our Bulk-Power System have already taken significant steps to protect critical facilities from physical attack. NERC's standards development process will benefit from the lessons learned from the owners and operators of the Bulk-Power System and the communication that will take place across the stakeholder community regarding physical security. However, I am concerned that the procedural approach chosen by the Commission will inappropriately preclude an open and transparent process in which all interested parties would be able to engage with the Commission as the standards development process gets underway. To limit communication and collaboration during the development of the standard has the potential to diminish our ability to achieve an optimal physical security standard. I believe the order does not sufficiently justify the uniquely expedited nature of the standard development process,

particularly when it will foreclose the Commission from engaging with stakeholders during that process. It would have been my preference to utilize an expedited rulemaking process for addressing this proposed reliability standard to allow the Commission to continue to engage with industry throughout the standard development process.

To ensure that all voices are heard, I encourage all parties to participate in NERC's standard development process to provide input regarding the appropriate approach for this standard. I similarly encourage all parties to participate in the rulemaking proceeding that will be initiated upon the filing of the proposed reliability standard at the Commission. Your voices, ideas, and experience are essential to the successful drafting and implementation of a reliability standard targeted to protect the physical security of critical facilities, the loss of which could result in instability, uncontrolled separation, or cascading failures. In addition, all parties should be mindful of the Commission's expectation that the number of critical facilities identified will be relatively small compared to the number of facilities that comprise the Bulk-Power System and should strive for balance between the measures related to physical security and the costs for consumers.

Second, I believe that our success in developing a comprehensive approach to addressing physical vulnerabilities relies at least in part on Congress taking steps to ensure the confidentiality of sensitive security information regarding the physical vulnerabilities of our grid. Currently, industry remains concerned that confidential security information submitted to the Commission would be subject to disclosure through Freedom of Information Act requests. These concerns have understandably left industry reluctant to provide the Commission with its most sensitive security information related to potential physical threats or vulnerabilities to our power grid. A reliability standard will likely have limited impact if industry, NERC, and the Commission remain unable to safely and securely exchange such information. Thus, I urge Congress to act expeditiously by creating a clearly-defined exemption to the Freedom of Information Act to allow for such exchange of information without fear of disclosure.

Third, I remain concerned that our recent efforts in ensuring the reliability of our transmission grid, both here and in other venues, have focused too narrowly on the need to bolster the physical security of our electric grid. I certainly believe that we must remain vigilant regarding grid security, as the security of our electric grid is essential to the health of our economy and the safety of all Americans. We should continue to take steps to bolster the physical security of our grid, and the reliability standard that we are directing here is a good step towards that goal. But, I also think it is important that we continue to equally focus our efforts, and our resources, on other threats to our nation's grid, including cyber-threats, geomagnetic disturbances, electromagnetic pulses, and natural disasters.

It appears to me that many people, both in the private and public sector, have rushed to address the need for physical security solely in response to the Metcalf incident. As I have said previously, I believe that incident is a serious one, and significant efforts should be made to determine who was responsible for the incident, and to identify appropriate next steps to prevent such incidents from happening in the future. But, it has been well understood for decades that our nation's grid has been vulnerable to physical attack. We simply cannot erect enough barriers to protect North America's over 400,000 circuit miles of transmission, and 55,000 transmission substations. While some locations may require additional physical barriers, I continue to urge caution against over-reaction. I remain concerned that the recent momentum will result in the electricity sector potentially spending billions of dollars erecting physical barriers to protect our grid infrastructure. I am particularly troubled because most if not all of those costs will be passed through to ratepayers.

I believe that the more prudent approach is to focus on building a smarter and more agile grid, incorporating better communication and coordination, to mitigate against the multiple forms of risks that we face, including as I stated above, physical and cyber threats, geomagnetic disturbances, electromagnetic pulses, and natural disasters. Such a multi-functional approach will enhance grid resiliency, which I believe is the best way to protect our grid from physical threats and vulnerabilities. A resilient grid should significantly limit the impacts of physical events, and potentially discourage future physical attacks, by ensuring that power will continue to flow to consumers even if certain elements of the grid are harmed.

The benefits of building a more intelligent and agile grid also goes beyond addressing resiliency and reliability. A modernized grid will enable us to more readily integrate intermittent resources, increase demand-side management capabilities, enhance the competitiveness of the wholesale energy market and more. The end goal to all of this should be to provide a more efficient grid that will provide long-term benefits to consumers in multiple ways.

For these reasons, I respectfully concur.

John R. Norris, Commissioner