March 2014

Issues Regarding the Development of NERC's Physical Security Standards
Can You Keep a Secret?

It may have come as a surprise to some that the current NERC[1] Reliability Standards do not contain specific physical security requirements for facilities that do not contain critical cyber assets.[2] That is not to say that physical security has been absent. To the contrary, many of the current reliability standards address physical security indirectly by focusing on preparation, prevention, and response and recovery efforts. This is called a "defense-in-depth" strategy that has been used by the industry for many years.[3] Nevertheless, it is not surprising, in light of recent attacks on important grid facilities, that regulators are looking to strengthen protection efforts in this area. Physical security measures, however, may be costly, especially if the new standards demand a hard-to-attain level of protection. The difficulty will be to find the appropriate level of physical security that can be tailored to provide reasonable protection for a variety of facilities with different threat and access levels.

Until recently, the subject of grid security and vulnerabilities has been kept out of the public eye, except for the relatively few, random vandalism incidents that occur across the country sporadically. There had been very little widespread public debate about the level of security, until the most recent incident involving the Metcalf facility in California and the subsequent article in the *Wall Street Journal* highlighting the nation's vulnerabilities.[4] NERC and Federal Energy Regulatory Commission (FERC) officials have expressed dismay, pointing out that such public statements about the level of physical security regarding grid facilities "do nothing to improve security, rather they jeopardize it."[5] Now that potential physical vulnerabilities of the grid are no longer best kept secrets, Congress and regulators have called for action.[6]

---

[1] North American Electric Reliability Corp.

[2] *Reliability Standards for Physical Security Measures, Order Directing Filing of Standards*, 146 FERC ¶ 61,166, P 5 (March 7, 2014) ("FERC Order").

[3] NERC Statement on Physical Security, March 13, 2014, http://www.nerc.com/news/Pages/Statement-on-Physical-Security,-Critical-Assets.aspx.

[4] *U.S. Risks National Blackout From Small-Scale Attack*, Wall Street Journal (March 12, 2014).

[5] NERC Statement on Physical Security, March 13, 2014; *see also* Statement of Acting Chairman Cheryl A. LaFleur On Publication of Wall Street Journal Article About Grid Security, March 12. 2014, http://www.ferc.gov/media/statements-speeches/lafleur/2014/03-12-14.asp ("the publication of sensitive material about the grid crosses the line from transparency to irresponsibility, and gives those who would do us harm a roadmap to achieve malicious designs.").

[6] Letter dated March 27, 2014, from US Senators Landrieu and Murkowski to the Department of Energy's Office of Inspector General, asking that an investigation be conducted to examine "apparent leaks" of sensitive and narrowly distributed FERC documents regarding physical threats to the nation's electric grid.

Development of New Physical Security Standards

In part in response to congressional pressure,[7] on March 7, 2014, FERC directed NERC to develop and propose new Reliability Standards to address physical security risks and vulnerabilities of the Bulk-Power System (BPS) facilities. Within 90 days, NERC must engage its stakeholder standard development process and draft and file for FERC approval new rules that require owners or operators of elements of the Bulk-Power System to identify and protect their "critical facilities." FERC defines critical facilities as 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."[8]

According to FERC, the new Reliability Standards should have three components. First, owners or operators of BPS facilities should conduct a risk assessment to identify their critical facilities. Although not mandating a specific type of risk assessment for all circumstances, FERC indicated that the risk assessment process should be based on objective analysis, technical expertise and experienced judgment to ensure that all critical facilities are identified. The assessment should also take into consideration any facilities that have a long lead time for repair or replacement, such as transformers, and elements of resiliency, such as the design, operation and maintenance of the grid, and the level of sophistication of recovery plans and inventory management.[9]

Second, the new Reliability Standards should require owners or operators of the identified critical facilities to develop methods for evaluating the threats and vulnerabilities to those facilities, taking into account the location, size and function of facilities as well as the relative attractiveness and vulnerabilities of those facilities as a target.

Third, the new Reliability Standards should require owners or operators of the identified critical facilities to develop and implement a security plan to protect the facilities against attacks.[10] The security plan does not need to dictate specific steps but it must provide an adequate level of protection against the identified potential threats. The end result will be that each owner or operator will have a plan that must be implemented and maintained. Compliance with the plan will be subject to NERC audit and penalties for noncompliance.

The standards development process at NERC normally has multiple rounds of drafting and options for stakeholder comments. The process typically takes significantly longer than 90 days to arrive at a proposed standard that is ready for a FERC filing. The process in this case will need to be fast-tracked and will provide much less time for stakeholder input. FERC emphasized that it is not looking for a "one-size-fits-all" solution to protect against physical security threats; however, several aspects of the rulemaking process will likely result in mandatory thresholds or minimum requirements that all owners or operators will have to follow.

Identification of "Critical Facilities"

FERC's order does not require that a mandatory number of facilities be identified as critical facilities.[11] FERC expects, however, that at a minimum, critical facilities will include critical substations and critical control centers. FERC indicated that it anticipates that the number of facilities identified as critical will be

[7] Letter to The Honorable Cheryl LaFleur, Acting Chairman, FERC, dated Feb. 7, 2014, from US Senators Ron Wyden, Harry Reid, Dianne Feinstein, Al Franken ("We are concerned that voluntary measures may not be sufficient to constitute a reasonable response to the risk of physical attack on the electricity system.").

[8] FERC Order at P 6.

[9] FERC Order at P 7. In addition, each entity's list of critical facilities should be verified by an entity other than the owner or operator that developed the list, such as NERC or a regional entity, and periodically updated. *Id.* at P 11.

[10] FERC Order at P 9.

[11] FERC Order at P 6.

small compared to the total number of facilities in the Bulk-Power System and that "most" substations, for example, would not be critical. FERC also indicated that it does not expect every owner or operator to have critical facilities. With such minimal guidance from FERC, several questions arise as to how critical facilities will be identified.

> **Will there be a voltage threshold for determining critical facilities?** The first step outlined in FERC's order is for owners and operators to develop a methodology/assessment framework for identifying critical facilities. What facilities will be considered critical facilities will necessarily be a system-by-system determination that will depend on many factors, such as the type of facility, its location, the state of the grid at that location, accessibility of the facility and the likelihood of its becoming a target. Developing a methodology that takes into account all these factors would appear to be the most appropriate methodology if it can be done in the 90-day time frame. In a similar, albeit more extensive, process, it took more than three years for NERC and FERC to establish a definition of the Bulk Electric System (BES). In the BES context, FERC was determined that a "bright line" voltage cutoff was necessary.[12] Because of time considerations in this proceeding, it may only be possible to outline some broad categories of facilities that would meet the definition, such as a voltage demarcation or facility type, such as substations.
>
> **Will critical facilities include transmission, distribution and generation facilities?** FERC's proposed definition of critical facilities is broad enough to include transmission, distribution and generation facilities. All these types of facilities, if damaged or destroyed, can have a critical impact on the operation of the interconnection through instability, uncontrolled separation or cascading failures on the Bulk-Power System. Thus, the types of owners and operators ultimately to be affected by the new standards includes a broad range of energy industry participants. Any owner or operator of BES facilities should pay close attention to this process and be prepared to provide input whenever necessary.

Cost and Liability Considerations

FERC's order makes no mention of cost as a consideration in developing the physical security plan that each owner or operator must have. Nor does FERC mention any means for cost recovery. Of course, the grid can be protected from just about any threat if the industry were willing to spend enough money to create fortresses or install armed guards around each critical facility. The same could be said for preventing power outages. However, as with preventing sporadic power outages, protecting the grid from all outages at all cost is simply not worth the cost. There needs to be some consideration of the cost of any physical security options adopted, to provide a reasonable balance between the risks posed and the cost to address them. The potential threats are limitless but ratepayer resources are not. It is difficult to predict the cost impact of any new standards that are developed and the costs will likely vary widely among owners and operators. For certain, the new standards have the potential to impose significant cost burdens.[13]

Liability considerations may also play a key role in the development of specific security standards. The more specific the standards are, the more companies will be subject to liability for noncompliance by regulators and third-party litigators. A company's conduct could be measured against the terms of potentially ill-fitting, one-size-fits-all regulatory standards instead of against what might be considered reasonable security measures on a utility-by-utility basis. There is also a potential for liability for failure to identify critical assets at the outset. Indeed, it may be only after an attack that assets initially considered to be noncritical are nevertheless found to have a significant impact on the grid when the facilities are rendered inoperable.

---

[12] *See North American Electric Reliability Corporation*, 146 FERC ¶ 61,199, P 4 (2014) (In November 2010, FERC first directed NERC to modify the then-effective definition of Bulk Electric System and that process still continues.).

[13] Statement of Commissioner John R. Norris re Physical Security of the Electric Grid, Feb. 20, 2014, https://www.ferc.gov/media/statements-speeches/norris/2014/02-20-14-norris.asp.

Time Frame for Physical Security Plan Implementation

Cost considerations aside, how quickly physical security measures must be implemented might also present issues to owners or operators subject to the new standards. FERC directed NERC to include time frames for implementing various aspects of the security plans, such as the risk assessments, threat and vulnerability assessments and the development and implementation of the plan. A short implementation time frame could present cost recovery issues for some owners or operators that may need regulatory approvals for operating cost increases.

Protecting Sensitive Information Regarding Critical Facilities

As mentioned above, publicity is no friend to grid security. Thus, if particular facilities are identified as critical, how will information about them be protected? FERC directed NERC to include in the new standards a proposed procedure to ensure confidential treatment of sensitive or confidential information but that would still allow FERC and NERC to have access to ensure compliance.[14] As with other NERC standards, compliance with the physical security standards will be mandatory and subject to periodic audits and possibly other reporting requirements. There will be numerous opportunities for information to be released to the public, whether or not intentionally.

Commissioner Norris commented separately that he expects that successfully developing an approach to address physical vulnerabilities depends in part on Congress's taking action to protect confidential security information and to address industry concerns that such confidential information would be subject to public disclosure under the Freedom of Information Act.[15] Commissioner LaFleur has also called for greater FOIA protections to protect sensitive grid security information.[16] Thus, a key feature of NERC's proposed standards must be strict information security requirements.

FERC Rulemaking Process

Although FERC cannot write reliability standards itself, FERC can reject standards proposed by NERC and direct NERC to make changes and propose new standards. Thus, after NERC's stakeholder process, FERC presumably will initiate a rulemaking process in which NERC stakeholders and other parties will have the opportunity to participate. During this process, FERC can accept NERC's proposed rules or direct that changes be developed and refiled. Given the unprecedented short time frame in which NERC has to make its initial proposal, it will likely be high level and nonprescriptive, leaving the details to the compliance stage. Once at the FERC rulemaking stage, parties that are not owners or operators, including politicians and parties with commercial interests in selling physical security hardware or services, will have the opportunity to call for stricter and more expensive measures that may have been previously considered and rejected. In addition, sending FERC a high-level standard proposal without sufficient detail runs the risk of FERC's rejecting it as vague or unenforceable as it did with the original version of NERC's CIP standards.[17]

[14] FERC Order at P 10; Statement of Commissioner Tony Clark re Securing Electric Grid Reliability, March 20, 2014, http://www.ferc.gov/media/statements-speeches/clark/2014/03-20-14-clark.asp.

[15] FERC Order, Commissioner Norris Concurring Statement.

[16] Letters from Acting Chairman Cheryl A. LaFleur, to US Senators Wyden, Reid, Feinstein and Franken, dated Feb. 11, 2014 ("Congress could improve the Commission's and NERC's ability to address the risks related to physical and cyber attacks by enhancing the confidentiality of sensitive security information concerning physical or cyber threats to, or vulnerabilities of, the bulk power system. A properly defined exemption from [FOIA] would be very helpful.")

[17] *Version 5 Critical Infrastructure Protection Reliability Standards*, 78 FR 24,107 (Apr. 24, 2013), 143 FERC ¶ 61,055, P (2013) (Notice of Proposed Rulemaking); 145 FERC ¶ 61,160, PP 35, 45-46, 65 (2013) (Final Rule).

Conclusion

Entities should pay close attention and provide input to the risk assessment and identification methodologies that will be incorporated into the new proposed reliability standards. Entities should also follow the FERC process once NERC's proposal is submitted because at that point the proposal will be subject to FERC's own review and to more subjective, political pressures that could drastically increase the standard requirements and resulting costs.

In the meantime, the industry and others should stop talking about specific grid vulnerabilities and the types of threats that could disable the grid and instead focus on ways to protect the grid at reasonable cost and keep sensitive grid security information out of the public eye.[18] In addition, we must keep in mind that intentional physical harm to the grid is only one of several threats that we should be concerned about, such as cyber-threats, geomagnetic disturbances, electromagnetic pulses, natural disasters and even human error.[19] As advocated by many industry experts, resiliency of the grid is where the focus should be, such as building a smarter and more agile grid that can better communicate and coordinate to withstand the multiple forms of risk it faces.[20]

Contacts

Linda L. Walsh
lwalsh@hunton.com

Ted J. Murphy
tmurphy@hunton.com

Paul M. Tiao
ptiao@hunton.com

C. King Mallory, III
kmallory@hunton.com

Mark W. Menezes
mmenezes@hunton.com

Kevin W. Jones
kjones@hunton.com

Frederick R. Eames
feames@hunton.com

Eric M. Hutchins
ehutchins@hunton.com

[18] Paul M. Tiao, *National Security at Risk Thanks to Disclosure of Grid Vulnerabilities*, IntelligentUtility Update, March 19, 2014.

[19] FERC Order, Commissioner Norris Concurring Statement.

[20] *Id.*