NERC Gains in Vegetation Management, Cyber and Physical Security, and Reliability Assurance

Deborah Carpentier

The North American Electric Reliability Corporation (NERC) recently issued its Annual Report, in which it set forth its 2013 achievements.[1] A few of the accomplishments stand out and are discussed below.

The North American Electric Reliability Corporation recently issued its Annual Report, in which it set forth its 2013 achievements.

VEGETATION OUTAGE EVENTS

Perhaps the most glowing report is that while there were 63 reported outages caused by vegetation growth into transmission lines in 2004–2010, only one has occurred in the last three years, and none in 2013. Ineffective vegetation management was identified as the major cause of the August 2003 blackout, which precipitated the establishment of mandatory reliability standards in the Energy Policy Act of 2005.

While there were 63 reported outages caused by vegetation growth into transmission lines in 2004–2010, only one has occurred in the last three years, and none in 2013.

NERC attributes this success to its formalized transmission vegetation management reliability standard, FAC-003. It requires a transmission owner to have a transmission vegetation management program that has the following:

- Establishment of "minimum vegetation clearance distance" (MVCD) between transmission lines and vegetation on and along rights-of-way, based, in part, on transmission-line voltage, ambient temperatures, and conductor sag
- Establishment of scheduled vegetation inspections, taking into account, among other things, expected vegetation growth rates
- Implementation of a program to control and remove vegetation that encroaches on the identified MVCD
- Quarterly reporting of outages caused by vegetation growing into lines or by vegetation falling into lines

Deborah A. Carpentier (dcarpentier@crowell.com) is a counsel in Crowell & Moring LLP's Environment, Energy & Resources Group. She focuses primarily on federal regulatory and transactional energy issues for electric utilities in matters before the Federal Energy Regulatory Commission and the North American Electric Reliability Corporation. This article is provided by Crowell & Moring LLP only for educational and informational purposes and is neither intended as nor should it be construed as legal advice. This article may be considered advertising under applicable state laws.

 DOI 10.1002/gas.21763

According to NERC, Version 3 of the standard, which has a staggered implementation starting July 1, 2014, will continue to promote "successful vegetation management programs" and "eliminate vegetation-related adverse impacts" on the transmission grid.[2]

The new version is expanded to include certain overhead transmission lines operated below 200 kilovolts and certain generator interconnection facilities. The new version also explicitly requires a transmission owner to prevent an encroachment into the MVCD. A violation will occur for the failure to do so regardless of whether that encroachment results in a sustained outage.[3]

And the new version requires a transmission owner to inspect annually all transmission lines subject to FAC-003 and to complete 100 percent of its annual vegetation work plan.[4]

CYBER AND PHYSICAL SECURITY

Following a NERC alert that detailed how common tools can be used to infiltrate critical infrastructure networks and gain access to control system networks, NERC, along with the Electricity Sector Information Sharing and Analysis Center (ES-ISAC), the Department of Homeland Security (DHS), the Department of Energy (DOE), and the Federal Bureau of Investigation (FBI), engaged in a series of briefings to raise awareness of these cyber threats.[5]

NERC also describes the physical security briefing series it undertook . . . to raise awareness of the threat of physical attacks on bulk electric system facilities in the wake of the 2013 shooting at the Metcalf transmission substation.

NERC also describes the physical security briefing series it undertook (in conjunction with ES-ISAC, DHS, FERC, and DOE) to raise awareness of the threat of physical attacks on bulk electric system (BES) facilities in the wake of the 2013 shooting at the Metcalf transmission substation. This major substation feeds power into the Silicon Valley. In this incident, high-powered rifles were used to knock out 17 transformers. At the time, power was rerouted and no major blackout occurred, but it took about a month to repair the damage.[6]

NERC officials did not believe that this incident caused the need for additional mandatory reliability standards to govern physical security. Gerry Cauley, NERC's chief executive officer, told various US senators the following:

> There are more than 55,000 substations of 100 kV or higher across North America, and not all those assets can be 100% protected against all threats. I am concerned that a rule-based approach for physical security would not provide the flexibility needed to deal with the widely varying risk profiles and circumstances across the North American grid and would instead create unnecessary and inefficient regulatory burdens and compliance obligations. (Letter from Gerry Cauley, president and CEO, NERC, to Harry Reid, majority leader, US Senate. [2014, February 12]. Retrieved from http://www.nerc.com/news/Headlines%20DL/NERC%20Response%20to%20Senators%20Letter%20-Reid%20%202%2011%2014%20v4.pdf [Cauley letter])

Rather, NERC believed that its outreach and awareness efforts have caused the industry "to further enhance their efforts to address physical security issues, and that significant investments are being made to address the risks related to physical and cyber security."[7]

Nevertheless, noting that physical BES attacks can result in instability, uncontrolled separation, or cascading failures, on March 7, 2014, FERC used its authority under Section 215 of the Federal Power Act to direct NERC to develop mandatory physical security reliability standards by June 2014.[8] FERC anticipates that these reliability standards would be applicable to only critical BES facilities, but each owner and/or operator of a BES facility would first have to do a risk assessment to determine whether such facility is critical—i.e., "is one that, if rendered inoperable or damaged, could have a critical

  / DOI 10.1002/gas

impact on the operation of the interconnection through instability, uncontrolled separation or cascading failures."[9]

There is some concern that FERC's directives in the Physical Security Order reflect an overreaction to the Metcalf incident. As noted, the lessons learned from the incident are being addressed through coordinated awareness and outreach efforts. Additionally, in NERC's Grid Security Exercise in November 2013 (GridEx), 2,000 individuals from all key BPS functions and relevant government agencies (e.g., DHS, FBI, and DOE) participated in a simulated cyber attack impacting corporate and control networks. A concurrent physical attack degraded reliability and threatened public health and safety.[10]

There is some concern that FERC's directives in the Physical Security Order reflect an overreaction.

GridEx exercised the readiness of industry and government to respond to coordinated cyber and physical attacks and identified potential improvements in industry programs, plans, and responder skills. NERC committees are now tasked with taking the recommendations from GridEx, which are set forth in the GridEx After-Action Report, to determine how best to act on them. Given that these efforts are already under way, the concern is that developing and imposing additional mandatory physical security standards would take resources away from other important issues NERC is addressing, including cyber threats, geomagnetic disturbances, and natural disasters.[11]

Moreover, additional physical security measures and the regulatory compliance mechanisms that are attendant to any mandatory reliability standard will undoubtedly increase costs. These will ultimately be borne by electricity consumers. For example, Pacific Gas and Electric Company (PG&E) announced that it would be upgrading security measures at the Metcalf substation, along with other PG&E facilities, including the installation of opaque fencing, advanced camera systems, enhanced lighting and alarms, and increased local police and security patrols.

PG&E noted that these measures could require a rate increase.[12]

RELIABILITY ASSURANCE INITIATIVE

NERC began the Reliability Assurance Initiative (RAI) in 2012 "to transform the current compliance and enforcement program into one that is forward looking, focuses on high reliability risk areas and reduces the administrative burden on registered entities."[13] The RAI was discussed in "Eliminating Zero-Tolerance Enforcement,"[14] and the major elements of RAI are not repeated here, but a few highlights from 2013 are discussed.

Under RAI, a registered entity can elect to develop and implement internal controls to reduce the compliance burdens of the entity's reliability standards. Such programs are subject to NERC's determination that the registered entity's internal controls allow the registered entity to self-assess risk and compliance and correct possible violations before such violations have a material effect on reliability. Where such internal controls are in place and where a self-reported violation does not pose a serious risk to reliability, the regional entity would then record the self-report without further investigation or enforcement. Registered entities have been concerned that developing or enhancing an internal controls program would add an additional level of review in the assessment of the internal controls and additional costs without a guaranteed benefit of reduced compliance burdens.

Entities have been concerned that developing or enhancing an internal controls program would add an additional level of review . . . and additional costs without a guaranteed benefit of reduced compliance burdens.

NERC recently addressed this concern. NERC noted that most registered entities currently have internal control programs and management activities in place that help them comply with reliability standards, regardless of whether they

 DOI 10.1002/gas

refer to them as internal controls. While registered entities do have these programs, the criteria by which NERC will judge whether such internal controls are effective so as to allow reduced compliance obligations are as yet unclear.[15]

That said, NERC has given some comfort to smaller entities that perhaps the demonstration of effective internal controls will not be a resource-busting exercise. NERC noted that the internal controls needed by a smaller entity should be "fewer and less complicated than those needed by a larger entity."[16] Therefore, the evaluation of a smaller entity's internal controls should be simpler. Moreover, whatever methodology is ultimately developed to evaluate internal controls should be "scalable to reflect the differences in internal controls needed by smaller and larger entities."[17] NERC thus concluded that "[b]y scaling the internal controls assessment methodology, the amount of effort required for smaller entities to organize and present their internal controls . . . should be significantly less than that required for larger entities."[18]

NERC has given some comfort to smaller entities.

Ultimately, however, NERC recognized that there is no "upfront guarantee of reduced compliance monitoring" prior to this assessment, and if a registered entity does not wish to go through the internal controls assessment, traditional compliance monitoring and enforcement will be used.[19] Consequently, although NERC has recognized the problem, until the assessment methodology is articulated and a determination is made that it truly is scalable, registered entities are still likely to be skeptical about whether the cost of demonstrating effective internal controls is worth the possibility of reduced compliance burdens.

Two other useful RAI documents that NERC developed in 2013 were user guides on mitigation plans and self-reports. Over the years, there has been much discussion about what elements should be included in mitigation plans and self-reports. These user guides are helpful in that they lay out with specificity what information needs to be included and why. The mitigation guide in particular provides very specific examples of information that is lacking and model information for each element of a mitigation plan. The self-report guide is notable in that it provides guidance on how to assess the actual and potential risks to the BES due to the possible violation addressed in the self-report.

Registered entities should review and train their compliance personnel on the content of these user guides, which are available on NERC's website.[20]

NOTES

1. NERC. (2014, February). *2013 annual report*. Retrieved from http://www.nerc.com/news/Headlines%20DL/NERC%202013%20Annual%20Report_final_web.pdf.
2. Ibid., p. 13.
3. FAC-003-3, Requirements 1 and 2. Retrieved from http://www.nerc.com/pa/Stand/Reliability%20Standards/FAC-003-3.pdf.
4. FAC-003-3, Requirements 6 and 7.
5. See Note 1, p. 23.
6. NERC. (2014, March 13). *Statement on physical security*. Retrieved from http://www.nerc.com/news/Headlines%20DL/Critical%20Asset%20Statement%2013MAR14.pdf.
7. Cauley letter (see p. 30).
8. Reliability Standards for Physical Security Measures, 146 FERC ¶ 61,166 (March 7, 2014) ("Physical Security Order").
9. Ibid., p. 6.
10. NERC. (2014, March). *Grid Security Exercise (GridEx II) After-Action Report*. Retrieved from http://www.nerc.com/pa/CI/CIPOutreach/GridEX/GridEx%20II%20After%20Action%20Report.pdf.
11. See, e.g., note 8 (Norris concurrence).
12. Avalos, D. (2014, February 10). PG&E plans to beef up security at substations in wake of attack. *San Jose Mercury News* (reporting that PG&E might have to seek a rate increase for enhancing physical security). Retrieved from http://www.mercurynews.com/pge/ci_25107368/pg-e-plans-beef-up-security-at-substations.
13. See Note 1, p. 15.
14. Carpentier, D. (2013). Eliminating zero-tolerance enforcement. *Natural Gas & Electricity*, 29(7), 30–32.
15. NERC. (2013, September 30). *Reliability Assurance Initiative (RAI) benefits and impact, Draft 1*, at p. 6. Retrieved from http://www.nerc.com/pa/comp/Reliability%20Assurance%20Initiative/RAI%20Impacts%20and%20Benefits%20V1.pdf.
16. Ibid.
17. Ibid.
18. Ibid.
19. Ibid.
20. These guides are available at http://www.nerc.com/pa/comp/Pages/Reliability-Assurance-Initiative.aspx. As of the date of this writing, these guides were not yet issued in their final form.

  / DOI 10.1002/gas