Portfolio Media. Inc. | 860 Broadway, 6th Floor | New York, NY 10003 | www.law360.com
Phone: +1 646 783 7100 | Fax: +1 646 783 7161 | customerservice@law360.com

Mounting Compliance Challenges Under New CIP Standards

Law360, New York (May 24, 2012, 1:03 PM ET) -- New criteria approved in April 2012 by the Federal Energy Regulatory Commission will impose cybersecurity standards on additional generating, transmission and other facilities critical to the bulk power system's reliability.

But complying with these standards by the July 2014 effective date is only part of the challenge presented by FERC's April 19, 2012, order approving Version 4 of the North American Electric Reliability Corp.'s (NERC) cybersecurity standards, known as the critical infrastructure protection (CIP) reliability standards.

Regulated entities must also prepare for the next version of the CIP standards, which FERC directed NERC to file by March 31, 2013, and the real possibility that Version 4 compliance efforts will be all for naught if the new cybersecurity standards are substantially revised before Version 4 ever goes into effect.

Background

FERC's Order No. 706, issued in January 2008, approved Version 1 of NERC's CIP standards but directed NERC to modify the standards to address several concerns, including the scope of regulated assets and the methodology for identifying these assets.

In response, NERC submitted, and FERC approved, Versions 2 and 3 of the CIP standards. But some Order No. 706 directives remained unaddressed.

Thus, in early 2011, NERC submitted Version 4 for FERC approval, which addressed some of the outstanding directives. Specifically, Version 4:

1. Provided "bright line" criteria for identifying "critical assets" subject to the substantive requirements of the CIP standards;
2. Identified associated violation risk factors (VRFs) and violation security levels (VSLs); and
3. Outlined a corresponding implementation plan.

NERC described Version 4 as an "interim step" designed to address the Order No. 706 directives.

FERC's April 19, 2012, Order

FERC approved Version 4, the proposed VRFs and VSLs, and the proposed implementation plan for newly identified critical assets and newly registered entities.

FERC reasoned that Version 4 would

1. Identify additional critical assets as compared to the number captured under Version 3;
2. Eliminate subjective, entity-defined, risk-based assessment methodologies that resulted in underreporting of critical assets; and
3. Provide more consistency and clarity to regulated entities.

Under the implementation plan, existing critical assets must be in full compliance with the CIP standards on the effective date of Version 4 — July 1, 2014. Newly identified assets and newly registered entities must comply in accordance with an implementation schedule set forth in NERC's proposal.

Reliability Standard CIP-002-4

CIP-002-4 reflects a significant departure from prior versions of CIP-002. It adopts 17 "bright line" criteria to identify critical assets, replacing subjective, risk-based assessment methodologies previously developed and used by regulated entities.

Version 4 maintains the initial and annual review of assets provided under Version 3 to ensure that new or modified facilities are timely identified and comply with the CIP standards.

The "bright line" criteria apply to facilities such as:

- Generating facilities totaling 1,500 megawatts (MW) or more at a single plant location;
- Reactive resources at a single location with an aggregate net reactive power nameplate rating of at least 1,000 megavolt-amperes reactive (MVAR);
- Generating facilities designated by a planning coordinator or transmission planner as necessary to avoid adverse reliability impacts in the long-term planning horizon;
- Blackstart resources identified in a transmission operator's restoration plan;
- Transmission facilities operated at 500 kilovolts (kV) or higher;
- Transmission facilities operated at 300 kV or higher at stations or substations interconnected at 300 kV or higher with three or more other transmission stations or substations; and
- Control centers and backup control centers performing reliability coordinator functions or controlling facilities covered by the new criteria.

FERC views the "bright line" criteria as a "regulatory floor." Registered entities can voluntarily apply any or all of the cybersecurity requirements or protections to assets that do not fall within the "bright line" criteria but that they deem to be critical. But assets not identified by the "bright line" criteria will remain outside the NERC cybersecurity compliance obligations.

As was the case under Version 3, after identifying its critical assets, a regulated entity must then identify its "critical cyber assets" associated with those critical assets.

To qualify as a critical cyber asset, the critical asset must:

1. Use a routable protocol to communicate outside an electronic security perimeter;
2. Use a routable protocol within a control center; or
3. Be dial-up accessible.

Finally, Version 4 made only ministerial, conforming changes to the remaining CIP standards (CIP-003 through CIP-009).

CIP Version 5

In the April order, FERC directed NERC to submit by March 31, 2013, Version 5 of the CIP Standards to address all remaining issues and directives under Order No. 706, as well as to submit quarterly status reports in the interim.

FERC also directed NERC to continue its efforts to eliminate the risk of "gaps" in identifying critical assets, including:

1. Addressing cyber connectivity and its potential to compromise reliable grid operations;
2. Considering relevant National Institute of Standards and Technology (NIST) standards in developing cybersecurity standards; and
3. Providing for external review in designating cyber assets as critical or recharacterizing the impact of cyber assets for compliance purposes.

Impact on the Industry

The newly adopted "bright line" criteria should provide the electric industry more consistency and uniformity in identifying critical assets. By design, the criteria also will sweep in more facilities subject to the CIP standards.

Surely compliance with the new CIP standards will increase cybersecurity protections and safeguards. But these benefits do not come without costs, such as hardware and software upgrades, compliance training and recordkeeping functions needed to comply, just to name a few.

Compliance with Version 4 — for both veterans and newly regulated entities — is further complicated by the anticipated approval and implementation of Version 5 looming on the horizon. An affected industry participant must engage in substantial planning and coordination across its enterprise to implement and comply with Version 4.

But Version 5 may render many of those compliance efforts moot if it overtakes Version 4.

Still, regulated entities should prepare compliance strategies with Version 4 in mind. While Version 5 is coming, entities should be wary of hedging their Version 4 compliance efforts on the arrival of Version 5.

To support effective and efficient compliance efforts, industry participants should participate in stakeholder processes and, if appropriate, seek guidance from NERC and FERC. Finding the right balance between achieving compliance and investing limited resources has never been more difficult, but hopefully doing so here will pay dividends with a more secure electric grid.

--By Daniel E. Frank, Meghan R. Gruebner and Jennifer J. Kubicek, Sutherland Asbill & Brennan LLP

Daniel Frank is a partner and Meghan Gruebner and Jennifer Kubicek are associates in Sutherland's Washington, D.C., office. The authors are attorneys in the firm's energy and environmental practice group.