Morgan Lewis

alert

energy lawflash

December 3, 2013

FERC Approves Version 5 CIP Reliability Standards, Rejects Key Reforms

The Commission rejects NERC's proposal to reform the existing "zero tolerance" to CIP compliance, describing the proposal as too ambiguous and unworkable.

On November 22, the Federal Energy Regulatory Commission (FERC or Commission) issued Order No. 791,[1] approving comprehensive revisions to the Critical Infrastructure Protection (CIP) Reliability Standards. The revisions were recently proposed by the North American Electric Reliability Corporation (NERC) to address many of the concerns regarding CIP compliance that have arisen over the last few years as well as to close out the remaining Commission directives ordering changes to the CIP Reliability Standards. However, although the Commission approved the substantive changes to the technical cybersecurity protection requirements contained in the proposed CIP Reliability Standards, the Commission rejected key reforms proposed by NERC, namely (a) NERC's proposal to end "zero tolerance" enforcement of the CIP Reliability Standards and (b) NERC's proposal to broaden the scope of assets subject to the CIP Reliability Standards but to impose only very minimal requirements for low-risk assets. As a result of FERC's order, the electric industry faces new, more demanding CIP Reliability Standards that lack some of the flexibility sought by the industry and NERC.

Order No. 791 approved the Version 5 CIP Reliability Standards, which contain revised versions of the currently effective CIP Reliability Standards, CIP-002-5 through CIP-009-5, as well as two new CIP Reliability Standards, CIP-010-1 and CIP-011-1, which take portions of the existing CIP Reliability Standards addressing change management, vulnerability assessments, and information protection and combine them into the two new standards.

Although the Version 5 Standards significantly rewrite and reorganize the existing CIP requirements to address clarifications and improvements identified since the CIP Reliability Standards were originally approved in 2008, the main focus of the order was on some of the major policy decisions proposed in the standards rather than the technical cybersecurity requirements they contain.

"Identify, Assess, and Correct" Language

The most significant policy change proposed by NERC in the Version 5 Standards, from a compliance and CIP practice perspective, was to direct utilities to implement the technical requirements in most of the CIP Reliability Standards in a manner that "identifies, assesses, and corrects deficiencies" in compliance. NERC had proposed this language to address the "zero tolerance" approach to CIP compliance that utilities currently face. Namely, all CIP Reliability Standards violations, no matter how small, low risk, or short in duration, are subject to compliance enforcement procedures that can be document intensive, time consuming, and expensive. By including the "identify, assess, and correct" language in 17 CIP Reliability Standards' requirements, NERC sought to provide some flexibility for utilities to minimize these compliance costs.

The Commission rejected this language and directed NERC to remove it from the standards within one year. According to FERC, the language was too ambiguous to permit the Commission to understand the obligations it imposes and could be subject to multiple interpretations. The Commission explained that it did support NERC's

1. View Order No. 791 at https://www.ferc.gov/whats-new/comm-meet/2013/112113/E-2.pdf.

attempt to move away from "zero tolerance" enforcement but that it was skeptical of NERC's effort to deal with the issue through language in a CIP Reliability Standard. The Commission explained that providing greater enforcement discretion and flexibility, while a laudable goal, is more appropriately addressed through changes to NERC's rules for enforcing compliance.

Compliance Requirements for Low-Risk BES Cyber Systems

The second major change introduced in the Version 5 Standards is to bring all Cyber Assets within the scope of the CIP Reliability Standards. Under the existing CIP Reliability Standards, only Cyber Assets related to particularly critical facilities are covered by the requirements in the standards. However, under Version 5, all "Bulk Electric System (BES) Cyber Assets" will receive some level of protection related to the importance of their associated facilities. To determine the level of protection required, utilities must first identify all of their "BES Cyber Assets" (a newly defined term), which are then grouped into "BES Cyber Systems" based on the reliability functional role they perform. Those BES Cyber Systems are then classified as High Impact, Medium Impact, or Low Impact using the bright-line criteria provided in CIP-002-5, which is based on the type of physical facilities the BES Cyber Systems are associated with, such as transmission control centers, transmission substations, and generating plants. The level of CIP protections required by the Version 5 Standards depends on the risk classification of the relevant BES Cyber Systems, with High Impact BES Cyber Systems receiving the most protections, Medium Impact BES Cyber Systems receiving slightly fewer protections, and Low Impact BES Cyber Systems receiving only a minimal level of protection.

The Commission approved this change, concluding that it will ensure more comprehensive protections for those Cyber Assets that affect bulk-power system reliability. However, the Commission rejected the vague protections proposed for Low Impact BES Cyber Systems. According to FERC, the requirement to protect these lower-risk assets by developing and implementing policies that address a handful of generically defined core cybersecurity issues, such as cybersecurity awareness, physical security controls, and incident response, fails to provide objective criteria on which the compliance and effectiveness of these security efforts can be measured. The Commission therefore directed NERC to develop modifications to the Version 5 Standards to provide for specific cybersecurity controls, objective criteria for evaluating the controls developed by utilities, or greater definition in the processes required under the existing proposal. Alternatively, NERC could propose another equally effective solution addressing the Commission's concerns.

For utilities subject to the CIP Reliability Standards, this creates an issue in that, whatever NERC's ultimate proposal, it will be stricter with regard to the CIP protections required for Low Impact BES Cyber Systems. Given the breadth of the assets captured in the "Low Impact" category (i.e., every bulk-power system–related Cyber Asset that is not Medium or High Impact), implementing a more demanding compliance program for those assets will likely require significantly more compliance work, with corresponding regulatory risk, due to the increasing possibility of noncompliance.

Implementation Plan Approved

In a victory for the industry, the Commission approved the implementation plan proposed by NERC. Under that plan, the Version 4 CIP Reliability Standards will not go into effect as scheduled. Instead, utilities will transition directly from the Version 3 Standards to the Version 5 Standards. Under the terms of the implementation plan, the requirements for High and Medium Impact BES Cyber Systems are effective 24 months after the effective date of FERC's order, and the requirements for Low Impact BES Cyber Systems will become effective 36 months after the effective date. As the effective date of the order is 60 days after publication in the *Federal Register*, which has not yet occurred, the effective date of the order should fall in the first quarter of 2014. That will require utilities to be compliant with the requirements for High and Medium Impact BES Cyber Systems by April 1, 2016 (the first day of the ninth calendar quarter after FERC approval). The sole requirement applicable to Low Impact BES Cyber Systems (CIP-003-5 Requirement R2), pending the changes noted above, will become effective on April 1, 2017 (the first day of the 13th calendar quarter after FERC approval).

Contacts

If you have any questions or would like more information on the issues discussed in this LawFlash, please contact any of the following Morgan Lewis attorneys:

Washington, D.C.

John D. McGrane	202.739.5621	jmcgrane@morganlewis.com
Stephen M. Spina	202.739.5958	sspina@morganlewis.com
J. Daniel Skees	202.739.5834	dskees@morganlewis.com

About Morgan, Lewis & Bockius LLP

With 25 offices across the United States, Europe, the Middle East, and Asia, Morgan Lewis provides comprehensive litigation, corporate, transactional, regulatory, intellectual property, and labor and employment legal services to clients of all sizes—from globally established industry leaders to just-conceived start-ups. Our international team of lawyers, patent agents, benefits advisers, regulatory scientists, and other specialists—more than 1,600 legal professionals total—serves clients from locations in Almaty, Beijing, Boston, Brussels, Chicago, Dallas, Dubai,* Frankfurt, Harrisburg, Houston, Irvine, London, Los Angeles, Miami, Moscow, New York, Palo Alto, Paris, Philadelphia, Pittsburgh, Princeton, San Francisco, Tokyo, Washington, D.C., and Wilmington. For more information about Morgan Lewis or its practices, please visit us online at www.morganlewis.com.

*In association with Mohammed Buhashem Advocates & Legal Consultants