Morgan Lewis

alert

energy lawflash

April 23, 2013

FERC Proposes to Approve Overhaul of NERC Cybersecurity Standards

Major revisions to the existing cybersecurity requirements for electric utilities will focus on greater protections for the most critical assets but will also ensure that all assets receive some level of protection.

On April 18, the Federal Energy Regulatory Commission (FERC) issued a Notice of Proposed Rulemaking (NOPR) that would approve version 5 of the North American Electric Reliability Corporation's (NERC's) Critical Infrastructure Protection (CIP) Reliability Standards.[1] The proposed rule aims to expand the scope of bulk electric system (BES) cyber systems protected by the CIP Reliability Standards. The proposal also includes 12 requirements with new cybersecurity controls as well as proposed modifications and clarifications to the CIP Reliability Standards. If approved, the revised CIP Reliability Standards will address a wider variety of utility computer systems and equipment, with the strictest protections applied to the most critical equipment.

Tiered Cyber System Classification

In Order No. 706,[2] FERC directed NERC to review the Risk Management Framework developed by the National Institute of Standards and Technology (NIST). Following its review, NERC proposed a NIST-like system to identify and categorize the impact BES Cyber Systems have on the reliability of the BES as a whole. BES Cyber Systems comprise cyber assets that are grouped together to perform reliability tasks and, if rendered unavailable, would affect the operation of the BES. Under the proposed system, these assets would be classified as "high impact," "medium impact," or "low impact" systems, based on their "reliability impact." The high-impact category covers large control centers, while the medium-impact category covers generation and transmission facilities and other control centers. The low-impact category covers all other BES Cyber Systems.

Under NERC's proposal, the utilities that are required to implement these requirements must maintain policies and specific implementation procedures for cybersecurity controls for both high- and medium-impact BES Cyber Systems. However, the compliance obligations for low-impact systems are more limited; these assets are only required to maintain general policy documents that provide guidance on compliance, as opposed to specific implementation procedures. FERC expressed concern over the more limited requirements for low-impact systems, stating the proposal would lead to inconsistent results and potentially insufficient protection for low-impact systems, and further directed NERC to adopt specific controls for low-impact systems.

Remaining Ambiguities

FERC also expressed concern over the enforceability of the CIP Reliability Standards, noting that language requiring responsible entities to "identify, assess, and correct" deficiencies was too ambiguous. FERC explained that this language is broad enough to be open to interpretation and that NERC's proposal does not explain the manner or time frame in which deficiencies should be identified and corrected or what constitutes a "deficiency." The resulting ambiguity, FERC stated, may contribute to confusion over the execution of the requirements, push disputes into future enforcement proceedings, and hinder subsequent audit efforts. FERC sought comment on

1. View the NOPR at https://www.ferc.gov/whats-new/comm-meet/2013/041813/E-7.pdf.
2. View Order No. 706 at http://www.ferc.gov/whats-new/comm-meet/2008/011708/e-2.pdf.

how this language would be implemented. This proposed language was an attempt to provide Registered Entities greater flexibility in detecting and remediating low-risk violations. With the move to version 5, many more cyber assets will be subject to the CIP Reliability Standards, and NERC recognized that using the full enforcement process for low-risk violations would be unworkable.

Implementation Schedule

NERC's original proposal regarding CIP Reliability Standards suggested that applicable utilities should transition compliance efforts from CIP version 3 directly to CIP version 5, thereby bypassing compliance with the recently approved CIP version 4. This would retire the version 4 CIP Reliability Standards before they could come into effect. FERC proposed to approve this plan but seeks comment on the mandatory implementation time line for the new version 5 CIP Reliability Standards. Specifically, NERC proposed a 24-month implementation period for high-impact and medium-impact BES Cyber Systems and a 36-month period for low-impact systems, but it did not provide a basis for this time line. Although FERC did not propose a specific alternative to NERC's time frame, it now seeks comment on the feasibility of implementing the version 5 CIP Reliability Standards on a faster schedule.

FERC is soliciting comments on the proposed rule, which must be submitted within 60 days after the NOPR is published in the *Federal Register*.

Related Developments

FERC's proposed approval of the new version 5 CIP Reliability Standards was issued on the same day the U.S. House of Representatives voted to pass the Cyber Intelligence Sharing and Protection Act (CISPA) for a second time. Originally introduced in 2011, CISPA faced resistance from the Senate and the White House due to concerns over privacy and information sharing. The legislation, which passed on April 18 in the House by a vote of 288–127, is designed to assist the U.S. government in investigating cyber threats and preventing cyber attacks on integrated network systems. As part of these efforts, CISPA would allow private companies to voluntarily share user data—potentially in real time—with the government to support deterrence of cyber attacks. The voluntary cybersecurity standards introduced by the bill have been widely criticized by privacy advocates, while supporters of the bill emphasize that the purpose of CISPA is to protect the critical cyber assets and infrastructures of private companies from malicious attacks. Although the bill will now make its way to the Senate, the White House has stated that President Barack Obama will veto the bill in its current form due to the lack of privacy protections.

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.

Stephen M. Spina	202.739.5958	sspina@morganlewis.com
J. Daniel Skees	202.739.5834	dskees@morganlewis.com

About Morgan, Lewis & Bockius LLP

With 24 offices across the United States, Europe, 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, 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.

outcomes. Links provided from outside sources are subject to expiration or change.