THE
NATIONAL LAW REVIEW

NERC Proposes New Protections for Low-Impact BES Cyber Systems

Morgan Lewis

Article By
J. Daniel Skees
Serge Agbre
Morgan, Lewis & Bockius LLP
Power & Pipes

- Communications, Media & Internet
- Environmental, Energy & Resources

- All Federal

Wednesday, March 29, 2017

Earlier this month, the ***North American Electric Reliability Corporation (NERC)*** submitted proposed changes to Reliability Standard CIP-003 to modify the cybersecurity protections required for low-impact BES Cyber Systems. In response to FERC's directives in Order No. 882, the new CIP-003-7 Standard (i) clarifies electronic access control requirements, (ii) adds requirements related to the protection of transient electronic devices, and (iii) requires utilities to have documented cybersecurity policies related to declaring and responding to CIP Exceptional Circumstances for low-impact BES Cyber Systems. The key changes are as follows:

Electronic Access Control Requirements

Utilities will be required to implement electronic access controls to permit only necessary inbound and outbound access to low-impact BES Cyber Systems for certain communications, whether direct or indirect, using routable protocols. This resolves the dispute regarding the existence of Low-Impact External Routable Connectivity (LERC) from an asset with a low-impact BES Cyber System, and the need to implement a Low-Impact BES Cyber System Electronic Access Point (LEAP) for the control of communications into the asset. Under the proposed standard, the LERC and LEAP concepts are discarded, and instead utilities are required to implement certain electronic access controls for all routable connections into and out of assets with low-impact BES Cyber Systems, regardless of whether those connections are direct or indirect.

Protection of Transient Electronic Devices

Under the proposed standard, utilities are also required to implement plans to protect transient electronic devices (e.g., laptops) with the goal of mitigating the risk of malicious code being introduced to low-impact BES Cyber Systems by, for example, a relay technician testing protection systems in a substation. The requirements differentiate between transient cyber assets managed by a utility and those managed by third parties such as vendors and contractors.

CIP Exceptional Circumstances Policy

NERC is also proposing changes that would require utilities to have policies for declaring and responding to CIP Exceptional Circumstances related to low-impact BES Cyber Systems. A CIP Exceptional Circumstance includes, among other situations, a risk of injury or death; natural disasters; civil unrest; imminent or existing hardware, software, or equipment failures; and cybersecurity incidents requiring emergency assistance. During a CIP Exception Circumstance, certain CIP requirements can be waived.

These revisions are the result of a lengthy stakeholder development process, and ultimately received strong support from the industry in stakeholder voting. The revisions also close the gaps in the CIP-003 Reliability Standard identified by FERC. As a result, the revised standard is likely to be approved by FERC. However, to the extent utilities have concerns over the substance or clarity of the proposed language, the upcoming notice and comment process at FERC will provide the last good opportunity to receive binding guidance from the Commission or challenge the language in the new standard.