Is Your Organization Prepared for Compliance With NERC Reliability Standards?

02.18.2010 | UPDATES

Compliance with the North American Electric Reliability Corporation (NERC) Reliability Standards, particularly the Critical Infrastructure Protection Reliability Standards (CIP Standards), can be challenging if not onerous. In addition, failure to comply with the standards presents potentially costly risks for companies involved in the generation, transmission and distribution of electricity. This Update discusses the scope of NERC reliability compliance and includes tips to help ensure compliance with the CIP Standards and other Reliability Standards.

WHAT ARE THE NERC RELIABILITY STANDARDS?

NERC was originally established in 1968 as the National Electric Reliability Council in response to major electrical blackouts in 1965 that impacted the Northeastern United States and Southeastern Ontario, Canada.[i] NERC's name and the scope of its authority have evolved over time. Recently, the U.S. Energy Policy Act of 2005 (EPAct 2005) authorized a self-regulatory electric reliability organization (ERO) that spans North America and is subject to Federal Energy Regulatory Commission (FERC) certification and oversight in the United States.[ii] EPAct 2005 gave FERC jurisdiction over the ERO and any regional entities that receive delegated enforcement authority from the ERO as well as all "users, owners and operators of the Bulk-Power System."[iii] EPAct 2005 also directed that compliance with the Reliability Standards be mandatory and enforceable.[iv]

In July of 2006, FERC certified NERC as the ERO to develop and enforce the Reliability Standards approved by FERC. All owners, operators or users of the bulk-power system—which generally include investor-owned and publicly owned utilities, generation and transmission cooperatives, and non-utility owners and operators of electric power generation, transmission or balancing facilities in North America (Responsible Entities)—must register with NERC and comply with the Reliability Standards. NERC and the eight regional entities have the obligation to identify and register all organizations that meet the criteria of a Responsible Entity, and NERC has developed criteria to evaluate whether a particular organization should be included in its registry.[v] In addition to certain other factors, an organization that meets certain functional performance criteria and is material to the reliable operation of the bulk-power system will be identified as a Responsible Entity and therefore subject to compliance with the Reliability Standards.[vi] Through its compliance program, NERC monitors, audits, investigates and has the authority to impose financial penalties of up to $1,000,000 per day per violation by a Responsible Entity of the Reliability Standards, subject to FERC review and oversight.

FERC has approved the first set of mandatory and legally enforceable Reliability Standards proposed by NERC (83 standards), with an effective date of June 2007.[vii] Of the 83 standards, many Responsible Entities have given special attention to eight standards that outline requirements concerning CIP Standards. The CIP Standards are designed to ensure protection of the bulk electric system by the Responsible Entities through various mandates, including directives governing the identification of critical cyber assets (certain electronic devices and other programmable assets critical to the operation of the bulk electric system), training for personnel with access to critical cyber assets, information protection, security of physical and electrical parameters surrounding critical cyber assets, testing and monitoring new critical cyber assets, and cyber security incident response and recovery plans. The CIP Standards have been problematic for many Responsible Entities, due in large part to ambiguity in the standards and the technical specificity involved in interpreting and understanding the standards. As of December 2009, few Responsible Entities had experienced a NERC audit of their compliance with the CIP Standards. However, many Responsible Entities are scheduled in 2010 for audits that will include audits of compliance with the CIP Standards.

TIPS TO HELP ENSURE YOUR ORGANIZATION IS “AUDITABLY COMPLIANT”

A Responsible Entity is required to demonstrate that it is “Auditably Compliant” with the applicable Reliability Standards selected for audit. “Auditably Compliant” means the Responsible Entity meets the full intent of the requirements in the standards and can demonstrate its compliance with them.[viii] In order to demonstrate such compliance, the Responsible Entity must, for most standards, furnish evidence that it has properly implemented and followed procedures that address the requirements of the Reliability Standards.

Compliance with the CIP Standards can be particularly challenging for Responsible Entities. The CIP Standards can, as noted above, be ambiguous and there is little available guidance. This can result in differing interpretations by Responsible Entities and auditors. Additionally, many of the CIP Standards may require implementing updated technology and outsourcing or hiring vendors to perform compliance tasks. Those actions can be expensive as well as time consuming for Responsible Entities. Finally, the CIP Standards have been in a state of flux, as NERC revises the standards in response to FERC orders on NERC's proposals.
Currently, the draft form of Version 4 of the standards is being finalized, and Version 2 has recently become effective. Many Responsible Entities will be audited against compliance with Version 1 of the CIP Standards, while at the same time they are drafting and implementing procedures to meet requirements in later versions.

The following are practical tips to help minimize the risk of a finding of noncompliance with the Reliability Standards:

- **Maintain a Culture of Compliance**
  Many Responsible Entities have successfully established a culture of compliance by creating and implementing an internal compliance program that includes procedures to achieve compliance with the Reliability Standards. Involving management and employees in development of the compliance program is key to garnering support for compliance with the requirements and an important step in establishing a culture of compliance and minimizing the risk of noncompliance with the Reliability Standards. For the CIP Standards, for example, this may entail ensuring that management is responsible for enforcing procedures regarding unauthorized access to physical security perimeters, ensuring that human resources adequately document personnel risk assessments for personnel with access to critical cyber assets, and ensuring that all employees are aware of the importance of protecting critical cyber asset information.

- **Watch for Guidance on Compliance With the Reliability Standards**
  Both FERC and NERC periodically publish guidance on compliance with Reliability Standards that describes various steps by which a Responsible Entity can demonstrate that it is Auditably Compliant. Through its administrative orders,[ix] FERC has published interpretations that provide insight into the intent and scope of many of the Reliability Standards. Guidance documents have also been published by NERC and are available on its Web site, often in response to FERC's orders for clarification. Additionally, although not officially approved by FERC, "FAQs" located on NERC's Web site provide helpful interpretations of NERC's CIP Standards. Many Responsible Entities have utilized these interpretations in creating and following CIP Standards compliance programs.

- **Plan Ahead for Presenting Your Compliance Documentation**
  As many Responsible Entities learned during audits of their compliance with Reliability Standards, gathering and organizing documentation of compliance can be challenging and time consuming. The Reliability Standards have varying data retention periods. Furnishing documentation to auditors during an audit requires planning and organization. As the CIP Standards become auditable, Responsible Entities will face new challenges in compiling and presenting documentation of compliance in electronic format, as required. Considering the best vehicle to display this documentation requires analysis and evaluation of technological considerations that may take time; planning ahead can minimize problems that may arise in gathering and presenting electronic evidence.

- **Legal Involvement in Your Compliance Program May Minimize Risk**
  Legal counsel can provide valuable insight and guidance as you prepare and implement your compliance program. For example, legal review of your procedures and programs designed to meet the requirements of the Reliability Standards can enhance the likelihood of establishing a culture of compliance. In addition, legal input regarding your compliance approach and evidence retention policies could result in mitigating the risk of noncompliance. Perkins Coie has assisted clients in developing Reliability Standards compliance programs and procedures and in preparing for compliance audits.

---

[i]  See http://www.nerc.com


Under EPAct 2005, Congress defined the bulk-power system to mean "(a) facilities and control systems necessary for operating an interconnected electric energy transmission network (or any portion thereof); and (b) electric energy from generation facilities needed to maintain transmission system reliability." The term does not include facilities used in the local distribution of electric energy. 16 U.S.C. § 824o(a)(1). In its Reliability Standards, NERC at times refers to both the bulk-power system and the bulk electric system with respect to its regulatory authority. The NERC glossary for its Reliability Standards defines the bulk electric system to include "the electrical generation resources, transmission lines, interconnections with neighboring systems, and associated equipment, generally operated at voltages of 100 kV or higher." See Glossary of Terms Used in Reliability Standards (Apr. 20, 2009). FERC has indicated that the terms are distinct, as Congress' definition under EPAct 2005 "does not establish a voltage threshold limit of applicability or configuration as does the NERC definition of bulk electric system." FERC has accepted NERC's definition of bulk electric system for now and may address any gaps in reliability due to the differing terms at a later date. Mandatory Reliability Standards for the Bulk-Power System, Order No. 693 ¶ 76-7, 18 C.F.R. 40 (Mar. 16, 2007). Further, despite proposed definitions by NERC, FERC has declined to adopt a more narrow definition of what "users, owners and operators of the Bulk-Power System" means. See Rules Concerning Certification of the Electric Reliability Organization; and Procedures for the Establishment, Approval and Enforcement of Electric Reliability Standards, Order No. 672, 71 Fed. Reg. 8662 (Feb. 17, 2006), order on reh'g, Order No. 672-A, 71 Fed. Reg. 19814 (Apr. 18, 2006).

 [iv]  16 U.S.C. § 824o(b)(1), 824o(e)(1). In addition, for reliability purposes, EPAct 2005 encourages coordination with Canada and Mexico. See 16 U.S.C. § 824o(h). Canada has long been a NERC participant, and NERC operating policies and planning standards became mandatory and enforceable in Ontario in May of 2002. NERC signed MOUs regarding its role as the electric
reliability organization in Canada with Ontario, Quebec, Nova Scotia and the National Energy Board of Canada in the fall of 2006.

[v] See Statement of Compliance Registry Criteria (Revision 5.0). The factors that will determine an organization's compliance vary, but include candidates with generation, transmission and interconnection operating at voltages of 100 kV or higher or load serving entities that have a peak load of 25 MW or greater and are directly connected to the bulk electric system or are designated as a responsibility entity as part of a required underfrequency load shedding program or a required undervoltage load shedding program. Id.

[vi] Id.


[ix] FERC orders may be viewed at www.ferc.gov.

CONTACTS

Pamela J. Anderson
Partner
Bellevue
D +1.425.635.1417

Donald G. Kari
Partner
Bellevue
D +1.425.635.1406

RELATED SERVICES

PRACTICES
• Energy Law
• Environment & Natural Resources
• Technology Transactions & Privacy Law