Fisher Insight

COMPLIANCE CHECK

Are your policies and procedures in line with NERC's latest requirements?

Once again, the North American Electric Reliability Corporation (NERC) has raised its security and reporting standards to keep electricity generation, transmission, and distribution companies on their toes. NERC recently updated or enacted three key requirements covering physical site security, cyber security, and disturbance monitoring and reporting.

If your company is registered with NERC, or you aspire to be, take note: NERC's job is to keep the electric grid secure and running consistently, so it regularly audits registered entities for compliance with its myriad of requirements. Penalties for noncompliance can be severe — to the tune of $1 million a day, in extreme cases — not to mention reputational harm or the potential to have your assets tripped from the system.

Here's what you need to know about the recent developments:

1. Physical Security Compliance

Transmission owners and operators who fit certain voltage class criteria are subject to Reliability Standard CIP-014-3, which is in place to identify and protect transmission stations, substations, and associated primary control centers which, if compromised by a physical attack, could result in widespread instability or disruption. CIP-014-3 modifies the compliance section of the previous version of this standard to eliminate a provision requiring that all evidence demonstrating compliance with this Reliability Standard should be retained at the owner's or operator's facility.

Affected owners and operators still must comply with the mandatory and enforceable requirements of this Reliability Standard, but they now have more flexibility in their choice of storage mechanisms to demonstrate compliance. NERC removed the facility-retention provision since it determined it wasn't necessary to protect confidentiality of the compliance evidence, and in practice it actually made compliance monitoring more difficult.

2. Cyber Security Compliance

Reliability Standard CIP-012-1 is now in effect. This cyber security protocol affects communications

(excluding oral communications) between control centers and is meant to protect the confidentiality and integrity of real-time assessment and real-time monitoring data transmitted between control centers.

Control center owners and operators deemed to be responsible entities within the standard center must implement documented security plans to mitigate the risk of unauthorized disclosure and unauthorized modification during such transmissions. The security plan needs to identify the nature of the security protection, where it is applied, and who is responsible for applying it if the control centers are owned or operated by different responsible entities.

3. Disturbance Monitoring and Reporting

Entities responsible for complying with PRC-002-2, the Disturbance Monitoring and Reporting Requirements, must now maintain 100% compliance with Requirements R2–R4 and R6– R11 of this standard, whose purpose is to ensure adequate data is available to facilitate analysis of Bulk Electric System (BES) disturbances.

This update follows the stepped implementation plan which allowed 50% compliance for some entities within four years of the standard's effective date, before requiring 100% compliance after six.

NERC Compliance the Fisher Way

Your enterprise can mitigate risk and avoid negative impacts with the Fisher Energy Team on your side. Let's talk about how our electrical engineering and design experts — which include a former NERC Audit Team Leader — can help you develop a NERC compliance program, assess your risk level, analyze compliance gaps, support you pre- and post-audit, and assist with your NERC 693 O&P program.

Ed Kostowniak, P.E., Director of Energy
716.858.1234 x313
EKostowniak@fisherassoc.com
Connect