Davis Wright Tremaine LLP

FERC Proposes to Remove Risk-Based Assessment Methodologies from Reliability Standards Relating to Cyber Security

By Brian R. Gish

September 19, 2011

The current mandatory reliability standard governing electric system cyber security requires each responsible entity to identify which of its assets are “Critical Assets” that support the reliability of the bulk electric system. The entity must make this identification by applying its own “risk-based assessment methodology” (RBAM). Many entities have struggled with how to perform such a risk-based assessment that would satisfy this reliability standard. FERC has now proposed to drop the amorphous RBAM concept in favor of bright line criteria.

Much of the electric industry is dependent on digital information being transferred through electronic pathways to control generators and transmission operations. These “cyber” pathways could be subject to deliberate or non-deliberate disruptions, potentially causing serious interruptions on the nation’s electric grid. The protection of cyber communications has been a matter of increasing concern within the electric industry.

The existing cyber security reliability standard was drafted by the North American Electric Reliability Corporation (NERC) and approved by the Federal Energy Regulatory Commission (FERC). NERC enforces mandatory electric reliability standards, which carry substantial monetary penalties for violations, for all entities that own or operate parts of the nation’s bulk electric system. A group of these standards address cyber security for “Critical Cyber Assets” and are designated as CIP-002 through CIP-009. Under this framework, the CIP-002 standard outlines the method for identifying Critical Cyber Assets, and the rest detail the requirements for protecting such assets. Such protection measures include security management controls, electronic security perimeters, physical security, incident reporting, and recovery plans.

The identification of which facilities qualify as Critical Cyber Assets has been one of the most difficult parts of the compliance obligation. Under the existing standard, this identification is a several step process with a fair amount of subjectivity. The first step is to identify which assets are “Critical Assets” that are needed to support the reliability of the electric system. This identification must be done by each responsible entity, e.g. each individual owner and/or operator of parts of the bulk power system, applying a risk-based assessment methodology that the entity chooses. The RBAM is applied annually to develop a list of its Critical Assets. The assessment must “consider” assets such as control centers, substations, generators, restoration systems, and any other assets that the responsible entity deems appropriate. After it has its list of Critical Assets, the responsible entity then must develop a list of the Critical Cyber Assets that are essential to control the Critical Asset. A senior manager of the entity must approve the risk-based assessment methodology and the list of Critical Assets and Critical Cyber Assets.

A number of entities subject to the CIP-002 standard did not know how to develop and apply a risk-based assessment methodology that would satisfy NERC. Many entities cannot determine whether their assets are critical to the operation of the electric system, because they lack the overview of how the power flows through the system in its region. FERC's Jan. 2008 Order approving the original standard fully recognized the inability of some entities to determine whether their assets were "critical," and directed NERC or its designee "to provide reasonable technical support to assist entities in determining whether their assets are critical to the Bulk-Power System."

In its Sept. 15, 2011 Notice of Proposed Rulemaking (NOPR), FERC proposes to adopt a revised standard developed by NERC for identifying Critical Assets under CIP-002. This new Version 4 of CIP-002 would jettison the whole concept of risk-based assessments, and substitute in its place 17 bright-line criteria that would tell an entity whether any of its assets are "critical." For example, Critical Assets would include a generating plant with an aggregate net power capability of 1500 MW or more, transmission facilities necessary to connect such a plant to the grid, reactive resources at a single location having an aggregate nameplate capacity of 1000 MVAR or greater, all transmission facilities operated at 500 kV or higher, control centers performing functions specified in the criteria, and other classes of assets. Presumably, if an entity has an asset that does not meet the criteria, the asset is not considered to be a Critical Asset, and would not need the cyber protection measures set forth in the reliability standard.

Aside from adding clarity to the definition of Critical Asset, FERC also notes that the proposed criteria would sweep more assets into the Critical Asset category than under the existing system. NERC provided data showing the increases in number of Critical Assets from the existing standard to the proposed standard. For example, the proportion of covered substations rated 300kV and greater would increase from 50% to 70%, and the number of control centers covered would increase from 425 to 553.

FERC asks for comment about whether the regulated entity and/or NERC should be allowed to identify assets as critical even though they do not meet the criteria. FERC also asks for comment as to how to better determine the cyber assets that are of most concern for protection. Further, FERC gives NERC guidance on areas that the standards need improvement, and proposes to give NERC until the second quarter of 2012 to address them. Comments are due on the proposed rule 60 days after it is published in the Federal Register.