
# Comments on Federal Energy Regulatory Commission Staff Preliminary Assessment of the North American Reliability Corporation's Proposed Mandatory Reliability Standards on Critical Infrastructure Protection (CIP-002 through CIP-009)

# Comments on

# Federal Energy Regulatory Commission
# Staff Preliminary Assessment of the

# North American Reliability Corporation's
# Proposed Mandatory Reliability Standards on
# Critical Infrastructure Protection
# (CIP-002 through CIP-009)

*(02/07/2007)*

**Executive Summary:**

The security experts at Aegis Technologies agree completely with the comments and observations in the FERC Staff Preliminary Assessment of NERC Reliability Standards, as published on December 11th, 2006. The FERC comments highlight key areas of concern that must be addressed to ensure a consistent and effective security infrastructure is put into place across various energy related organizations and systems. Without carefully crafted standards that address issues, viable security policy and practice capable of withstanding a coordinated nationwide attack is not possible.

In addition to the FERC Staff Preliminary Assessment, Aegis Technologies offers the following comments and suggestions. We hope these ideas may be useful to the process of improving and extending the Reliability Standards to a level which results in effective security and protection of our Nation's Critical Infrastructure.

**Items for Consideration:**

**1.0 Viability of End-To-End Security – Templates from Other Business Sectors**

Any statement that a complete end-to-end security infrastructure is impossible to achieve, or would be too costly, should be considered with scrutiny. The Banking Sector is an example of an industry that has successfully implemented complete end-to-end security across their systems, and also between financial institutions. Because of the financial nature of their business, defense in depth can be found at all layers of the banking infrastructure, from end-user interaction on the web to internal processing to intra-bank and international money transfers. Such measures have been adopted industry wide by banking entities, and continuous evaluation and standards processes produce improvements to the existing security models in place.

Perhaps risk assessment, policies, and security models in use in the Banking Sector may provide a useful template for application within the Energy Sector. Aegis Technologies is successfully

deploying security technology within the Energy Sector, based on security primitives used within the Banking Sector. These security technologies not only interoperate well with Energy Sector systems, but also provide viable end-to-end security across a wide range of technology platforms and disparate systems. Suffice it to say that viable security frameworks already exist from within other industries, and that these could be adopted with little modification, or at least used for comparison to, proposed solutions for the Energy Sector.

**2.0 Clarified Scope of Reliability Standards – Bulk Electric System**

As already noted by FERC, the proposed reliability standards specify only a limited guidance on the scope of the standards.

In addition to clarifying scope of the term "Responsible Entity", an update to the Reliability Standards could go a long way toward properly defining this scope by providing an explicit definition of "Bulk Electric System." The FERC Staff Preliminary Assessment uses the term "Bulk Power System". For this discussion, both phrases, "Bulk Electric System" and "Bulk Power System" are treated as having same meaning.

Although protection of the "Bulk Electric System" appears to be the goal of the Reliability Standard, the reader's own imagination must come into play to determine what systems and processes are meant. For example, it is unclear if small utilities or operators have infrastructure that is part of the "Bulk Electric System." Also, in the case of a large utility or operator, it is unclear if auxiliary non-energy related systems (e-mail, file servers, Internet connections) are included in scope of the "Bulk Electric System."

As noted by FERC, past bodies have declined to specify the scope of "Bulk Power System", and the Reliability Standard follows this model by specifically not defining "Bulk Electric System."

The lack of definition and scope of either of these terms seems only to add to existing confusion among entities that are be considering whether or not they must comply with the Reliability Standards. The Reliability Standards could be substantially improved by providing a concise and clear definition of the scope of these terms.

Since a seemingly small attack can have a ripple effect that has a larger effect on energy delivery, a reasonable and effective cyber security approach for most business entities is to secure ALL connected system components within the entity's sphere of control. Non-energy related business entities often choose to do this by securing all outside connection points with a firewall or a similar technology, and by implementing secured and authenticated communications for all connections to outside entities. For critical applications, additional layers

of security are implemented at application, database, server, and network technology points. Additional intrusion detection and prevention systems may be in place. Defense in depth is a key here. This is a reasonable approach followed by many business entities as a means of preserving the entity's ongoing business interest in the face of a cyber-threat filled environment.

For the purpose of enhancing the Reliability Standard, from a security standpoint, it's recommended that the term "Bulk Electric System" and "Bulk Power System" be defined to include all systems within the entity's domain of operation and control, that have a direct or indirect, electrical or wireless connection with systems and networks that support generation, transmission, distribution and final delivery of energy resources. In short, everything connected directly or indirectly to energy systems must be *at least considered* in the Risk Assessment.

This scope may seem large, but the simple fact that the Risk Assessment includes all of the above systems and equipment can help ensure that no obvious technology systems are missed during the assessment. And the simple definition of scope itself helps clarify what systems and networks must be considered, who the Responsible Entities are, and improves the overall consistency of application of the Reliability Standard.