
# FERCs Preliminary Assessment of the NERC CIP 002 – 009 Cyber Security Standards Aegis Technologies Comments

**FERCs Preliminary Assessment of the NERC CIP 002 – 009 Cyber Security Standards**
**Aegis Technologies Comments**

## Abstract

After four years, numerous drafts and three name changes (Urgent Action Cyber Security Standard 1200, Cyber Security Standard 1300, and Critical Infrastructure Protection 002 – 009), NERC has adopted security standards (effective June 1, 2006) for the "Bulk Electric System". It should also be stated that these standards were developed by industry members.

FERC issued its staff preliminary assessment of the adopted standards in a document dated December 11, 2006. The purpose of this assessment was to analyze the CIP 002 – 009 Standards and comment on them. The assessment was limited to a technical review and makes no determination on whether the standards satisfy statutory and regulatory criteria.

FERCs approach was to use the strategy of "defense in depth" to analyze cyber threats. Defense in depth involves layering of various defense mechanisms in a way that either discourages an adversary from continuing an attack or creates hurdles. FERC believes that the key to success of any set of cyber security standards is that they provide reliable direction on how to choose among alternatives to achieve an adequate level of security.

Effective cyber security standards must have a reasonable balance. They cannot be too specific which would lead to a "one size fits all" solution, but they must have sufficient specificity that will provide useful direction to the Responsible Entities.

FERC assessed each of the individual CIP Standards in detail. The assessment was very comprehensive and identified several areas of importance in each standard where inadequacies or deficiencies exist. Many of these inadequacies/deficiencies were the result of insufficient specificity in guidance, range of methodologies allowed to the Responsible Entities, and the applicability of the standards.

## FERCs Three Common Concerns

The assessment and comments identified three common concerns pertaining to all of the CIP 002 – 009 Standards:

- Discretion and Business Judgment
- Defining Compliance
- Applicability

We agree with all the FERC comments that were given under these three categories and would like to emphasize some specific areas of concerns:

- Discretion and Business Judgment: We strongly agree that the level of flexibility and discretion allowed in the interpretation of the CIP Standards undermines their effectiveness. All eight of the standards begin with the statement that the Responsible Entity should interpret and apply the standard using "reasonable business judgment". This language allows for a broad interpretation of each standard which will result in varying levels of cyber critical asset identification, implementation, measurement, auditing and compliance of the standards. The CIP Standards give a Responsible Entity too much latitude in deciding how secure they need to be.

In addition, CIP-002 states that this standard requires the identification of Critical Cyber Assets through a "risk-based assessment methodology". We strongly agree with FERC that this first standard is the key to achieving a successful framework and affects the implementation of the remaining standards. However, with no real guidance given, and leaving the identification methodology up to the individual Responsible Entity, the result of asset identification will vary significantly with each Responsible Entity. This will result in weak links in the chain. **Our belief is that any device connected to the communication control system network is vulnerable or is potentially vulnerable.**

For the purpose of CIP 002, Critical Cyber Assets are further qualified to be those having at least one of the following characteristics: 1) the asset uses a routable protocol to communicate outside the Electronic Security Perimeter; or 2) the asset uses a routable protocol within a control center; or 3) the asset is dial-up accessible. Does this mean that NERC wants to exclude serial-based protocols from the standards? It could be interpreted that way. However, all serial protocols are connected to the Front End Processor which has a routable protocol. In addition, is NERC implying that securing traditional serial-based protocols (i.e. DNP3, Modbus, Conitel, CDC, etc.) is either impossible or not economically feasible to be included in the standards? Or do they not see that these protocols have a security concern? **The medium and method may be different, but the vulnerability of the system with either still exists.**

There are no requirements to protect information being sent from one "discrete" entity to another "discrete" entity. In most cases, that information is critical in nature or could be confidential customer-related information and should be included in any security policy or standard.

- Defining Compliance: We agree with FERC that "the most critical element of a Cyber Security Standard is the Requirements" because they will define what a Responsible Entity must do to be compliant and establish an enforceable obligation. However, all of the CIP Standards allow too much flexibility and discretion in identifying "exceptions" or areas where the Responsible Entity can document instances where they cannot conform to the cyber security policy. This documentation need only be authorized by a "senior manager of delegate". **What constitutes a senior manager or delegate?** Many of these exceptions are identified as processes or controls that are "technically feasible". Security technology required to comply with the standards have evolved considerably over the past several years and exist today (encryption, device and user authorization, authentication, intrusion detection, firewalls, audit and monitoring processes, etc.) to speed the CIP compliance effort. There should be no exceptions given based on a required technology not being available from a vendor. We also strongly agree with FERC that the auditable compliance timetable extends too far.

  Several standards allow the Responsible Entity to "accept risk" rather than meet one or more of the standard's requirements. Since there is so much grid interconnectivity, one Responsible Entity accepting a risk is essentially accepting the risk for the other Responsible Entities connected to that grid. Those Responsible Entities who have fully complied with the CIP Standards will be accepting risks of other Responsible Entities without knowing it. Think back to the Northeast blackout of 2003. This is an concern that would be very important to stockholders of the Utilities. Security concerns should not be predicated only regarding the occurrences of September 11th. This concern is emphasized further in the Applicability section below.

- Applicability: NERCs stated mission is to ensure the reliability and security of the bulk electric system. The term "bulk electric system" is used in the first paragraph (Purpose) of CIP 002, Cyber Security Asset Identification. It specifically states that "NERC Standards CIP 002 – 009 provide a cyber security framework for the identification and protection of Critical Cyber Assets to support reliable operations of Bulk Electric System". Subsequent paragraphs in this standard state that the standards "recognize the differing roles of each entity in the operation of the Bulk Electric System, the criticality and vulnerability of the assets needed to manage Bulk Electric System reliability, and the risks to which they are exposed." This begs the question, "What is NERCs definition of the Bulk Electric System?" Based on the language above, some entities may interpret that they are too small to be included in these standards. Other entities may interpret that they are excluded. If the mission of NERC is to ensure the reliability and security of the nation's electric grid, **all entities, small or large, must be included and categorized as a Responsible Entity**. A chain is only as strong as its weakest link. We agree with FERCs assessment that **"it is not the size of an entity that is critical but rather the potential for an entity to become a vector of vulnerability to the security posture of interconnected control systems".**

**Summary**

We believe that FERC has identified several deficient areas of the NERC CIP 002 – 009 Cyber Security Standards. They have correctly noted that there is not enough specific direction provided to the Responsible Entities to develop, implement and manage an effective cyber security policy. There is far too much discretion and flexibility allowed in implementing procedures to comply with a policy.

FERC has identified a security strategy they call "defense in depth". We believe that they did not go far enough in the definition of this strategy. FERC highlighted this approach by identifying defenses such as firewalls, intrusion detection systems, audit logs, etc., but it does not mention encryption. Encryption ensures the confidentiality of data exchanges, and up to a point, their integrity. We realize that encryption by itself should not be looked at as the only security measure deployed within a cyber security strategy - but without it, a security strategy cannot be viewed as comprehensive or complete.

While we understand that the drafting team of the NERC CIP 002 – 009 Standards had to deal with many complex challenges, we believe they intended to be very general in writing and adopting the standards. We believe they thought it would be much easier to achieve consensus among their peers and that any standards would be better than none. However, being compliant to general requirements does not ultimately achieve the initial intended goal of the standards – a secure electrical grid. **From a solution providers point the CIP 002 – 009 Cyber Security Standards, as written, do not provide a bar to reach or exceed or the incentive to develop the greatest level of innovation in a product solution**