

FERC Staff Issues Preliminary Assessment of NERC's Proposed Critical Infrastructure Protection Reliability Standards

NERC Standards Would Impose New Requirements On Senior Management

January 3, 2007

On December 11th, Staff of the Federal Energy Regulatory Commission (FERC or Commission) issued a "Preliminary Assessment" of the North American Electric Reliability Corporation's (NERC) proposed mandatory reliability standards governing critical infrastructure protection (CIP). The CIP reliability standards developed by NERC and its working groups primarily address cyber security and, if approved, would require users, owners, and operators of the Bulk Power System (Responsible Entities) to develop and implement a number of cyber security measures. Certain proposed CIP standards require the direct involvement of senior management.

The Preliminary Assessment recommends that the proposed standards have wider applicability, provide less discretion to Responsible Entities, and contain better-defined compliance requirements. **Comments on the Preliminary Assessment and NERC's proposed CIP reliability standards must be filed with the Commission on or before February 12, 2007.**

Background

The Energy Policy Act of 2005 amended the Federal Power Act (FPA) to address the creation of a system of mandatory and enforceable reliability standards for the nation's Bulk Power System. Specifically, section 215 of the FPA authorizes the Commission to approve mandatory and enforceable reliability standards, including cyber security measures. NERC filed its proposed CIP reliability standards with the Commission on August 28th, 2006. The Commission intends to address the proposed CIP standards in a forthcoming rulemaking proceeding in Docket No. RM06-22-000.

FERC Staff's General Concerns

The Preliminary Assessment identifies a number of overarching concerns common to many or all of NERC's proposed CIP standards. These concerns include the following:

- **Business Judgment.** FERC Staff acknowledges that Responsible Entities must have some flexibility to implement cyber security standards. Staff is concerned, however, that the proposed standards provide too much discretion. In particular, Staff is concerned that language contained in each standard – "Responsible Entities should interpret and apply the Reliability Standard using reasonable business judgment" – unduly compromises the effectiveness of the CIP standards and will undermine enforcement initiatives. The Preliminary Assessment concludes that "invoking the reasonable business judgment rule appears out of place in the context of mandatory Reliability Standards."
- **Defining Compliance.** The Preliminary Assessment found that many of the proposed CIP reliability standards only provide limited general direction in terms of defining adequate cyber security practices. FERC Staff suggests that compliance requirements set forth in the CIP standards contain more specificity.
- **Implementation Compliance.** NERC proposes that Responsible Entities should not be required to be "Auditably Compliant" until the second quarter of 2009. FERC Staff asserts

A Professional
Corporation

1050 Thomas Jefferson
Street, NW
Washington, DC
20007-3877
(202) 298-1800
(202) 338-2416

The Millennium Tower
719 Second Avenue
Suite 1150
Seattle, Washington
98104
(206) 623-9372
(206) 623-4986

www.vnf.com

I
S
S
U
E



A
L
E
R
T

that it may be possible to assess a Responsible Entity's level of compliance prior to achieving "Auditably Compliant" status.

- **Applicability.** The Preliminary Assessment challenges the notion that some entities are too small to have a material impact on the Bulk Power System. FERC Staff asserts that small entities generally should be required to comply with NERC's CIP standards because the assets and operations of a smaller entity may provide a gateway to compromise larger entities and, in the aggregate, have an adverse impact on the Bulk Power System. FERC Staff also raises concerns that the CIP standards will not be applicable to NERC, a Regional Entity, or a Regional Reliability Organization because these entities may not be characterized as users, owners, or operators of the Bulk Power System.

Assessment of Proposed CIP Standards

NERC's proposed CIP standards include seven cyber security standards and one physical security standard. The Preliminary Assessment raises the following concerns with each of the specific standards:

1. CIP-002-1. Critical Cyber Asset Identification. CIP-002-1 requires Responsible Entities to develop a risk-based assessment methodology for identifying critical assets. Once developed, the Responsible Entity must identify those associated cyber assets that qualify as critical cyber assets essential to the operation of critical assets. *This proposed standard requires senior management to approve, and annually reevaluate, the list of critical assets and critical cyber assets.* The Preliminary Assessment raises concerns over the scope of the critical asset assessment, the timing of updates, and the ability of certain entities to determine that they have no critical assets or critical cyber assets. FERC Staff also recommends that senior management be required to approve any risk assessment methodology utilized by a Responsible Entity.
2. CIP-003-1. Security Management Controls. CIP-003-1 requires Responsible Entities to develop and implement cyber security policies and procedures. *This proposed standard requires senior management to lead the cyber security program and to conduct an annual review of security policies and procedures.* The Preliminary Assessment questions the lack of specific requirements with regard to cyber security polices, allowable exceptions to adopted security policies, and the ability of Responsible Entities to accept the risk of non-conformance with certain security policies.
3. CIP-004-1. Personnel and Training. CIP-004-1 requires Responsible Entities to establish a cyber security training program and a risk assessment program for all personnel having access to critical cyber assets. The Preliminary Assessment questions the lack of specificity with regard to the elements of the security program, the criteria for assessing the quality and adequacy of training, and the ability of untrained personnel to have access to cyber security assets for up to 90 days.
4. CIP-005-1. Electronic Security Perimeters. CIP-005-1 requires Responsible Entities to establish an electronic security perimeter to encompass all critical cyber assets, develop vulnerability assessments, and conduct testing. The Preliminary Assessment takes issue with the reliability standard's focus on the documentation of the mapping of assets; FERC Staff recommends that this standard instead address the adequacy of the mapping and perimeter identification. FERC Staff also questions whether the requirements of this standard should be conditioned on "technical feasibility" as currently proposed.
5. CIP-006-1. Physical Security of Critical Cyber Assets. CIP-006-1 requires Responsible Entities to create and maintain a physical security plan to ensure that all cyber assets within an electronic security perimeter also reside within an identified physical security perimeter. *The physical security plan must be approved by senior management.* The Preliminary Assessment recommends: (a) that the physical security plan include actions to be taken in response to a physical security breach; (b) more timely updates of the security plan; and (c) expansion of the requirements governing document retention.

6. CIP-007-1. Systems Security and Management. CIP-007 -1 requires Responsible Entities to define methods, processes, and procedures for securing systems identified as critical cyber assets, as well as non-critical assets within an electronic security perimeter. The Preliminary Assessment challenges the “acceptance of risk” standard that would allow Responsible Entities to avoid undertaking certain security measures. Similarly, FERC Staff questions whether implementation of certain security tools if “technically feasible” provides too much discretion to Responsible Entities.
7. CIP-008-1. Incident Reporting and Response Planning. CIP-008-1 requires Responsible Entities to develop and maintain Cyber Security Incident Response Plans. The Preliminary Assessment seeks better-defined criteria for a “reportable incident” and recommends specific time frames for reporting cyber security incidents.
8. CIP-009-1. Recovery Plans for Critical Cyber Assets. CIP-009-1 requires Responsible Entities to develop, update, and test recovery plans for critical cyber assets. The recovery plans must follow established business continuity and disaster recovery techniques and practices. The Preliminary Assessment seeks comment on aspects of the standard related to the backup and storage of information, the timing associated with recovery plan updates, and the description of triggering events.

For Additional Information

If you would like additional information on FERC Staff’s Preliminary Assessment or NERC’s proposed reliability standards, or seek assistance in developing comments on the CIP reliability standards, please contact Jay Ryan, Gary Bachman, Cheryl Feik Ryan, or any member of our Electricity or Infrastructure Security practices at (202) 298-1800 or www.vnf.com. A copy of FERC Staff’s Preliminary Assessment is posted at www.vnf.com/security.

#

Founded in 1977, **Van Ness Feldman** helps clients in a variety of industries achieve their business goals by designing and complying with the nation’s energy and environmental laws. Many of the firm’s more than 80 attorneys and public policy professionals served as chief legal counsel to key congressional committees and Members of Congress; high-level officials in the Department of Energy, the Federal Energy Regulatory Commission, the Environmental Protection Agency, The White House, and the Department of the Interior; or as high-ranking officers in major trade associations.