

**To:** Gerry Adamski, NERC, Vice President and Director of Standards

**From:** Kathleen Goodman, Senior Operations Compliance Coordinator  
Joseph Pereira, Cyber-Security Manager  
Matthew F. Goldberg, Director, Reliability & Operations Compliance

**Date:** April 10, 2009

**Subject:** ISO New England voting comments on Project 2008-06, Cyber Security Standards

As you are aware, ISO New England (ISO-NE) is committed to maintaining and supporting high-quality, enforceable, mandatory Reliability Standards -- a part of which includes the Cyber Security Standards. We have, however, two fundamental enforceability-related concerns with the currently-posted draft. We believe that these concerns warrant a Negative vote. The Standards at issue are CIP-003, R2 and CIP-006, R1.6.

To the extent that NERC could sever these two provisions from its filing of the CIP Standard modifications to the Federal Energy Regulatory Commission ("FERC"), or alternatively, FERC (under 18 C.F.R. §39.5(e)) could disapprove, in part, these two aspects of the CIP Standard modifications, ISO-NE would otherwise vote in the Affirmative for these CIP Standard modifications.

**A. CIP-003, Requirement 2**

Under the Standards as currently drafted (*see specifically* CIP-002), ISO-NE has a single senior manager responsible for approving annually the list of Critical and Critical Cyber Assets. That list has been developed pursuant to a risk-based methodology adopted by the ISO-NE. Under ISO-NE's current management structure, business units (in this case the Information Services Department) are responsible for identifying Critical Cyber Assets. Other Departments with key responsibilities – such as setting the ISO's budget and capital expenditures (as is the case of the Finance Department) – also play a role in ensuring that the Company can implement needed steps to comply. As explained further below, it is difficult to understand how the newly proposed Requirement 2 of CIP-003 has a reasonable relationship to defining or improving upon a "reliability" or "security" objective.

Requirement 2 of CIP-003 states "Leadership — The Responsible Entity shall assign a single senior manager with overall responsibility and authority for leading and managing the entity's implementation of, and adherence to, Standards CIP-002-2 through CIP-009-2." There are numerous problems with this new requirement.

**1. The Requirement Does Not Appear to be a Reliability Standard.**

First, this requirement appears to overstep the authority granted to NERC as the ERO under Section 215 of the Federal Power Act in that it attempts to dictate “how” a responsible entity meets compliance with a reliability/security objective – in this case how the company establishes a management structure to achieve compliance. This requirement sets no actual “reliability” or “cybersecurity” performance requirement, and therefore appears to have no reasonable relationship to NERC’s authority to set “reliability standards” as that term is defined under Section 215. “Reliability Standards” are “requirement[s] for the operation of existing bulk-power system facilities, including cyber-security protection.” **Attempting to dictate, in this instance, how companies organize their management goes well beyond NERC’s authority to establish standards governing the “operation” and “protection” of bulk-power system facilities.**

FERC has previously recognized the distinction between regulating “what” registered entities need to do, as opposed to regulating “how” they achieve those reliability/security objectives, and the need for the ERO to balance these considerations. *See* Order No. 672 at P260. By establishing a Standard that seeks to regulate internal management structure without explaining how such a requirement itself establishes greater security, the proposed modification would not appear to address the need to balancing “what” is being regulated versus “how” it is accomplished. **More generally, the entire enforcement regime helps to ensure that companies are doing what is necessary to implement standards. No specific requirement is needed stating as much.**

**2. The Standard Drafting Team Provided No Suitable Rationale as Concerns a Non-Reliability or Security Matter.**

Second, even if this matter is argued to be within NERC’s authority, the Standard Drafting Team provided no suitable justification explaining its purpose. ISO-NE, and other entities, raised this concern in prior comments, and the Standard Drafting Team (“SDT”) simply deferred to generic language in Order No. 706. *See, e.g.*, Order No. 706 at P381 (the “Commission’s intent is to ensure that there is a clear line of authority and that cyber security functions are given the prominence they deserve.”). *See also* U.S. – Canada Power System Blackout Task Force, Final Report on the August 14, 2003 Blackout in the United States and Canada: Causes and Recommendations (April 2004) (Blackout Report), Recommendation 43 (recommending that corporations establish “clear authority” for physical and cyber security, and that this “authority should have the ability **to influence** corporate decision-making and the authority to make physical and cyber security-related decisions.”) (emphasis added).<sup>1</sup>

However various parties or regulators might interpret what constitutes suitable “influence”, achieving the Commission’s intent on ensuring that cyber-security matters are given “prominence” within a Responsible Entity could be accomplished in a variety of ways **other than** drafting new Standard requirements. Such other measures could include the manner in which NERC requires periodic reporting by responsible entities, the frequency with which NERC could conduct audits of responsible entities, etc.... In fact, the whole scheme of establishing a phased-

---

<sup>1</sup> *See* <http://www.ferc.gov/industries/electric/indus-act/blackout/ch7-10.pdf>

in approach for the CIP Standards acts as a means of ensuring that NERC and Regional Entities *track* Responsible Entities' progress in meeting the Standards – itself a metric for measuring the “prominence” with which the implementation of Standards is given within a Responsible Entity.

The concept of “authority and implementation” – as drafted by the SDT for inclusion as a mandatory *Standard* – simply does not add much to what the FERC and the Blackout Report has previously observed. However, when drafted as a Standard, the language raises issues of: (a) how the SDT intends this requirement to be interpreted, (b) the ERO's specific intent under Section 215 of the Federal Power Act behind approving a requirement that regulates management structure, and (c) how Regional Entities, NERC or FERC would enforce such language.

More generally, it is well understood that SDT may explore a variety of means to address the FERC's concerns. In this instance, given the authority issues raised by NERC Stakeholders, the SDT should have provided more rationale of its proposal. It is especially important for the SDT to provide a robust rationale for its decisions if it attempts to regulate non-technical matters, because FERC is only obligated to give “due weight” to the “technical expertise” of the ERO when determining when to approve a Standard or Standard modification. *See* 18 C.F.R. § 39.5(c)(1). As importantly, given the fact that ERO determinations of a non-technical nature might have *broader* impacts to how other Standards are developed or modified, understanding the thinking of this particular SDT is necessary to ensuring future standards are drafted appropriately.

### **3. Ambiguity in the Standard Suggests that NERC Intends Responsible Entities to Assign Too Much Authority with One Individual.**

As noted above, while the provision itself attempts to address generally expressed concerns in Order No. 706, it also appears to envision a management structure that could be at odds with generally accepted principles of corporate management.

While the phrase “overall responsibility and authority for leading and managing the entity's implementation of, and adherence to” compliance with standards might be susceptible to multiple interpretations, it could unduly “blur the lines” between key Business Officers (for example, between Information Services and Finance as concerns the language relating to “implementation of” compliance). “Implementation” of these standards may involve decisions regarding authorizing capital expenditures, and these decisions may not be within the authority of any specific business unit/manager. These decisions may involve the functions of a Chief Finance Officer or even a Company's Board of Directors, in which case the “overall responsibility and authority” **cannot** sit with a single individual.

Of course, the SDT may have a different concept in mind when it referred to a single individual having “responsibility” and “authority”, but the SDT never gave a fulsome explanation of what it had in mind, and *how it was implementing the issues raised in Order No. 706*. **This vagueness should establish real concerns about how this “standard” will be enforced.**

### **4. Drafting Creates Potential Confusion with Other Standards.**

Finally, even if the provision is a justifiable exercise of NERC's authority, ISO-NE believes this requirement is poorly drafted as it should be contained within, and harmonized with, CIP-002. Under CIP-002, some Registered Entities will find that the CIP-002 through -009

requirements do not apply. Moreover, because CIP-002 refers to “a senior manager” having responsibility for approving the Critical and Critical Cyber Asset list, placing this new provision in CIP-003 simply creates unnecessary confusion in how to apply multiple provisions that relate to the same thing in different standards.

### **B. CIP-006, Requirement 1.6**

Requirement 1.6 of CIP-006 states “Continuous escorted access within the Physical Security Perimeter of personnel not authorized for unescorted access.” Of course, under the current version of the Standard, ISO-NE provides “escorted access” through a variety of means, such as through providing physical escorts and through installing electronic surveillance at access points. Because of the ambiguity regarding “continuous,” ISO-NE believes additional information is needed that would support the enforceability/measurement of compliance with the Standard and what is actually needed to implement further measures to ensure compliance. This is particularly important to ISO-NE, because it needs to present its budgeted capital expenditures to its stakeholders for review and advice.

First, with regard to the enforceability, ISO-NE is concerned that “*continuous*” escorted access will prove to be a difficult, if not impossible, Requirement with which registered entities can effectively demonstrate compliance, because of the difficulty determining what records/data can show that such escorting was “uninterrupted.”

Second, further information is needed about what “continuous” means, because of the need to develop an appropriate implementation plan to carry out such a requirement. For example, if a company has multiple visitors on site, then the measures employed to ensure “continuous” escorting for each visitor can rapidly increase. For example, if there are multiple personnel working within the Physical Security Perimeter, each one would appear to need a separate escort.

While ISO-NE believes that the concerns raised above warrant continued work on **this requirement** before it should be approved, ISO-NE requests, in the alternative, additional guidance/clarification on how to interpret what constitutes a “continuous” escort.

### **C. Conclusion**

As stated above, ISO-NE takes its CIP Standard compliance very seriously and supports the development of improved CIP Standards. ISO-NE believes that the Standards proposed for approval here, if omitting the Requirements identified above, would themselves establish a more robust CIP Standard regime.

The concerns identified with only these two requirements above were made during the comment period of the drafts now being balloted. In ISO-NE’s view, these concerns have not been sufficiently dealt with by the SDT to produce an enforceable, auditable product. A more robust explanation from the SDT might have served to address ISO-NE’s concerns, but lacking that, ISO-NE is compelled to raise its objections again at this time. We look forward to working closely with the SDTs in the future to ensure high-quality Standards for protecting the bulk-power system’s reliability and cyber-security and enabling robust enforcement.

April 10, 2009

Page 5 of 5

cc: Jamshid Afnan  
Vamsi Chadalavada  
Bob Ludlow  
Gordon van Welie