ISO new england

memo

To: Mr. Gerry Cauley
Vice President and Director of Standards
NERC

From: Kathleen Goodman

Date: March 24, 2006

Subject: ISO New England comments on the Recirculation Ballot on the Cyber Security Standards (NERC CIP-002-1 through CIP-009-1)

ISO New England strongly supports the initiative to provide industry controls for security of Critical Cyber Assets. The existing Urgent Action (1200) Cyber Security Standard requirements represented a major first step for the industry to take in regard to providing cyber security for our Critical Cyber Assets.

However, ISO New England cannot support adoption of the proposed new Standards without further consideration of industry comments and concerns previously offered through the comment and balloting process, reinforced here.

Our concerns are categorized into the following:

(a) Extensive focus on documentation versus true improvements to security: ISO New England is concerned that the requirements focus primarily on documentation and less on the substantive changes that will result in increased security. For example, the levels of non-compliance do not fairly reflect the potential impact on the reliability of the grid, but instead imposes penalties simply for not having documentation. This focus on meeting administrative requirements instead of meeting a higher level of security/reliability seems contradictory to the spirit of adopting a Cyber Security Standard.

(b) Considerable ambiguity in the Standards: The developed standards rely heavily on the FAQ's to clarify the intent, exemplifying the fact that the Standards, as written, remain open to a wide range of interpretation. We understand that the FAQ's are intended to be adopted as a NERC reference document. However, ISO New England strongly believes that a NERC Standard should be understandable and enforceable based on its face. For instance, CIP-007, Requirement 8, Cyber Vulnerability Assessment, was interpreted in two different ways: (1) the FAQ indicates an annual port scan must be conducted to meet this requirement of the Standard; while (2) the responses to "no votes with comments" indicates that a comprehensive assessment of all assets is necessary to meet this requirement of the Standard.

ISO New England Inc.
One Sullivan Road, Holyoke, MA 01040-2841
www.iso-ne.com **T** 413 535 4111 **F** 413 535 4343

(c) Cost-benefit analysis: ISO New England is concerned that the costs of this standard will outweigh the benefits. This belief stems from the concerns outlined above and the examples cited below.

Example 1: In the responses to "no votes with comments", there is a requirement to perform an annual comprehensive vulnerability assessment of all assets within the electronic security perimeter. This creates an additional burden with minimal increase to the security of the assets internal to the perimeter. Performing such vulnerability assessments on assets within the perimeter is also a potential risk for inadvertent failures of critical assets needed to perform reliability functions.

Example 2: Minimizing access to the Critical Cyber Assets through physical and logical access provides the most benefit to the protection of Critical Cyber Assets. However, the extensive documentation and retention of logs required to assert proof of such protection, provides little, if any, security but requires much more resources than is really necessary to ensure security of these Assets.

Example 3: The need to review "unauthorized access attempts" immediately "upon discovery". The resources required to verify the potential false positives (i.e. battery failure on an authorized access card, an authorized employee accidentally alarming a reader simply by physical proximity to the reader and not an actual attempt at entry) on a daily basis in unreasonable because there may have been no actual attempt at a security breach.

Example 4: The "revocation of authorized access within 24 hours" for vendor personnel. If an ISO New England vendor is terminated by their employer and ISO New England is not notified, it remains ISO New England's responsibility for not meeting the 24-hour revocation requirements. The only way to ensure compliance with this is for the entire industry to rework all contracts and hope the vendors adhere to them.

These are impractical requirements, costly, and do not necessarily increase security.

While ISO New England strongly believes and supports the need for a Cyber Security Standard and generally believes there are positive attributes embedded in these Standards, we believe they require further refinement and clarification prior to industry adoption.

Cc: Gordon van Welie
Jamshid Afnan
Peter Brandien
Kathleen Carrigan
Vamsi Chadalavada
Donald Gates
Chuck Noble
Joe Pereira
Stephen Rourke
Michael Taniwha
Stephen Whitley

ISO New England Inc.
One Sullivan Road, Holyoke, MA 01040-2841
www.iso-ne.com **T** 413 535 4111 **F** 413 535 4343