REQUEST TO APPROVE PROPOSED CYBER SECURITY STANDARD

Dear Registered Ballot Body Member:

I am writing to solicit your approval of the proposed urgent action cyber security standard, which will be posted for ballot from May 12-21, 2003. A team of industry experts from the Critical Infrastructure Protection Advisory Group (CIPAG) developed this standard. As chair of this team it is my belief, and the belief of these experts, that the reliability of the bulk electric systems of North America may suffer if this standard is not approved. Because threats to cyber security can impact electric system reliability, the Standards Authorization Committee (SAC) unanimously authorized the use of the urgent action procedure contained in NERC's *Reliability Standards Process Manual*.

It is important that you ensure Information Technology management for your organization is aware of the proposed standard. Your IT professionals for computer and network management and information security are the people who will carry the most responsibility for implementation. Their review and advice on its affects and benefits should be considered in determining your vote on this standard.

Justification for Urgent Action Procedure

- The interconnected nature of the bulk electric system requires all entities whose operations can affect the operation of the bulk electric system to be as secure from cyber incidents as practicable to ensure bulk electric system reliability.

- On January 25, 2003, the SQL Slammer Worm was released by an unknown source. The worm significantly disrupted many Internet services for several hours. It also adversely affected the bulk electric system controls of at least two entities. These events have been studied in detail. No unintentional control actions and no service interruptions occurred due to these events; however, both entities lost their ability to execute bulk electric system control from their primary control centers for several hours. Those who have studied these incidents believe that at least one would have been prevented had the actions set forth in the proposed standard been taken.

- In February 2003, the President's Critical Infrastructure Protection Board stressed the urgent need to improve the cyber security of the nation's infrastructure:

  > *A spectrum of malicious actors can and do conduct attacks against our critical information infrastructures. Of primary concern is the threat of organized cyber attacks capable of causing debilitating disruption to our Nation's critical infrastructures, economy, or national security.*
  >
  > *The cyber security of large enterprises can be improved through strong management to ensure that best practices and efficient technology are*

being employed, especially in the areas of configuration management, authentication, training, incident response, and network management.[1]

- Within the last month the U.S. government released an advisory stating that a group of hackers are planning extensive, coordinated cyber attacks.

- The FBI notes that there were 82,094 reported cyber incidents in the year 2002. This number exceeds the total of all cyber incidents that were reported in prior years.

- A number of electricity sector organizations have stated they are receiving 200 or more credible intrusion attempts per month.

I believe the consequences of the Slammer Worm incident in January 2002 effectively point to the potential risks to the electric industry of inadequate cyber security. It is also clear that some electricity sector organizations have not sufficiently secured their cyber assets, particularly assets that may be critical to the support of reliable electric system operations.

I do not envision a single, large "Pearl Harbor" type of event affecting our industry. But I do envision a significant increase in frequency, from one or two major cyber attacks per year, to two or more per month, using multiple attack methodologies simultaneously. With the ongoing war on terrorism and the current war in IRAQ, it is critical that the electric industry take all practicable steps, as soon as possible, to ensure that those whose operations may affect the bulk electric system meet a minimum threshold for the security of their critical cyber assets.

The industry must start to close its cyber security vulnerabilities now. I do not believe that we can wait for cyber security standard to be developed through the regular NERC standard development process. I consider it an unacceptable risk to allow known cyber security vulnerabilities to exist for two or more years, without redress, in the face of increasing threats.

An Internet Webcast will be conducted on May 5, 2003, to formally present the proposed cyber security standard and provide the industry with an opportunity for questions and comments. You and your IT professionals are invited to participate in this Webcast. The specifics of this webcast will be communicated to you shortly. Attached to this letter is a list of questions and responses designed to address questions you may have about the proposed standard and the process used for approving it. Please share this letter and the attached document with your IT professionals.

---

[1] "The National Strategy to Secure Cyberspace," The President's Critical Infrastructure Protection Board, February 2003. The report contains detail in support of the proposed standard; it is available at http://www.dhs.gov/interweb/assetlibrary/National_Cyberspace_Strategy.pdf .

The electric industry has an opportunity to shape its own future by adopting responsible cyber security standards. The threats are real, as is the need to take action. If the industry does not take advantage of this opportunity, it is entirely possible that either the federal government or a number of states will seek to develop and impose their own requirements for cyber security standards. Your approval of this urgent action security standard will be an important first step in achieving a more secure and reliable infrastructure for bulk electric system operations.

Thank You,

Charles E. Noble, CISSP
Information Security
ISO New England