Oral Testimony

Good afternoon Mr. Chairman, Ranking Member McCall, and Members of the Committee. I would like to thank the Committee for your commitment to a comprehensive examination of the cyber security of control systems utilized in our nation's electric grid. I also want to thank you for the opportunity to be here today to discuss this very important topic.

I am a nuclear engineer that has been involved in control systems for over 35 years and control system cyber security for over 7 years. I have been a part of the NERC cyber security standards process since its inception. I have been working with government organizations, end-users, equipment suppliers, domestic and international standards organizations, and others to develop standards and solutions. I am also a utility shareholder and ratepayer, both of which can be affected by this subject.

The issue at hand is the protection of the interdependent critical infrastructures of electric power, water, oil/gas, etc. Control systems form the backbone of these infrastructures and the threat of a cyber attack is the central issue. There are only a handful of control system suppliers and they supply industrial applications worldwide. The control systems, architectures and default passwords are common to each vendor. Consequently, if one industry is vulnerable, they all could be.

I am aware of more than 90 cases where control systems have been impacted by intentional and unintentional cyber incidents. These incidents have occurred in electric power transmission and distribution systems, power generation including fossil, hydro, gas turbine, and nuclear, water, oil/gas, chemicals, paper, and agri-business. Damage from cyber incidents have ranged from trivial to significant environmental releases, to significant equipment damage to even deaths.

When the NERC cyber security standards process originated, it was meant to address utility control systems with the only exclusion being mainstream business applications.

Over time, the scope significantly narrowed. The approach has resulted in the following shortcomings:

- The ambiguousness and exclusions of the NERC CIP process - telecom, electric distribution, market systems, serial communications, nuclear plants, and not requiring appropriate policies - would not meet a cyber security assessment of a Human Resources computer system, yet we are using it as a basis for our most important critical cyber assets.
- The banking industry is concerned about the security of a single open access point on a laptop. On the other hand, the electric industry has determined by using the NERC CIP standards that an entire section of the United States has no critical generation assets. How can this be considering NERC's input on the Aurora vulnerability?
- In my written testimony, I have provided 4 actual control system cyber events the NERC CIP standards would not have addressed including one identified by the Electric Sector ISAC in 2003 (not Aurora).

As can be seen, this lack of any real security being addressed by NERC is alarming at best and negligent at worst. This begs the question- what is the point of the NERC CIPs - an effort to placate FERC or to actually secure the grid?

There is a better approach that in fact is already mandatory for all federal agencies which includes TVA, BPA, the Bureau of Reclamation, among others. This approach is the NIST Framework which has been extended to specifically address control systems. We conducted a line-by-line review between the NERC CIPs and NIST 800-53. The results were that NIST SP800-53 is more comprehensive. Why should federal power agencies be held to a higher standard, but more so, be placed at risk where non-federal agencies connect with them using a less comprehensive approach. Again, this makes no sense.

Recommendations

Congress should empower FERC with the authority and responsibility for development of control system cyber security requirements and compliance criteria similar to the role of the Nuclear Regulatory Commission. In so doing, Congress should also provide FERC

with the authority to separate ERO functions so that NERC is responsible for traditional electric system reliability standards, and have a separate organization, such as ISA, be responsible for the cyber security aspects of critical infrastructure protection. Finally, Congress should take action so that the ERO function is funded by the government, not by industry as is now the case, to better ensure that conflicts of interest do not interfere with doing what is right and necessary and not just what is convenient.

Thank you for allowing me to provide my thoughts and concerns. I would be happy to answer any questions.

Joe Weiss
10/17/07