September 23, 2005

EnergyPulse™
Insight, Analysis and Commentary on the Global Power Industry
http://www.energypulse.net

NERC CIP Compliance: It's Time to Start Covering Your Assets!

Network & Security Technologies

Adam Lipson, President and CEO, Network & Security Technologies, Inc.

Ratification of the North American Electric Reliability Council (NERC) Critical Infrastructure Protection standards for Cyber Security (NERC CIP-002-1 through CIP-009-1) should occur in early 2006. When complete, these will affect nearly all companies and organizations within the electric power industry. Most will find that the new, permanent requirements significantly expand the scale and scope of the earlier NERC Urgent Action Standard 1200 – Cyber Security. More importantly, NERC will receive official recognition by FERC as the ERO (Energy Reliability Organization) enabling it to levy monetary penalties for non-compliance. Only immediate action and careful planning can effectively mitigate these liabilities.

But, how can an organization begin work on a standard still in draft form?

Much of the NERC CIP standards exist already. (Check out the NERC website http://www.nerc.com/~filez/standards/Cyber-Security-Permanent.html for Draft 3 and ancillary documents.) These represent a reorganization of the NERC 1200 standards. They extend the requirements and measures of the original, as well. But, the starting point for both entails identification of all cyber assets requiring protection.

The NERC CIP-002-1 diverges from NERC 1200 by requiring Responsible Entities to begin with a list of their Critical Assets (e.g., power plants, substations and control centers). Once this is done, the organization must then identify and document the Critical Cyber Assets “essential to the reliable operation of Critical Assets.” (The original standard started with the cyber assets, not the critical ones.) Importantly, the identification method must follow a documented, “risk-based assessment” process.

Every Responsible Entity will begin its compliance efforts with this asset identification process. They will have to establish their own “risk-based” criteria that correspond to their unique position in the grid. Thus, they should work with experts both inside and outside the organization to develop and document their set of criteria. This makes an excellent starting point for many to immediately begin their compliance efforts.

The majority of affected organizations have a control center and backup control center that qualify as Critical Assets. The computers and networks that provide the data and information to

drive decisions made in the control center are, therefore, Critical Cyber Assets. Today's complex control center environment means that many systems support the control center activities. Even if the control center is the only Critical Asset, it will likely lead to a substantial list of Critical Cyber Assets.

However, other organizations will have a much longer long list of Critical Assets. These will include generation plants, substations, special protection systems, load shedding equipment, system restoration pathways and other components that support the Bulk Electric Grid. For all of these, the Responsible Entity must identify the cyber assets "essential to the reliable operation of Critical Assets." This includes both data acquisition and system protection equipment. In their initial compliance work, these organizations should identify all potential cyber assets and develop their Critical Cyber Asset list from them.

Many can turn to existing NERC compliance documentation for a good starting point. Specifically, NERC 1202 – Critical Cyber Assets states that Responsible Entities "shall maintain a document identifying critical cyber assets." Later guidance from NERC suggested that this only applied to cyber assets contained within the SCADA aggregation points. It excluded remote devices in substations such as relays and RTUs. Organizations that demonstrated NERC 1200 compliance should already have an up-to-date list of Critical Cyber Assets at their control centers. Yet, for both organizations that did not participate in NERC 1200 and those that did, listing assets outside control centers will pose a significant challenge. While the standard limits the definition of Critical Cyber Assets to those that use dial-up connections or a routable protocol, the potential coverage will still be significant.

Estimating the work required to achieve NERC CIP compliance will require accurate lists of Critical Assets and Critical Cyber Assets. These will require the participation of personnel from all facets of the organization including generation, transmission, operations, telecommunications and system support. All Responsible Entities, regardless of their size, need to start the process of creating these lists now and documenting their process for future compliance efforts. Waiting for full ratification may be too late. FERC's oversight of NERC's role as the ERO may put mandatory compliance on a fast track. By then, time will be short to create an accurate Critical Cyber Asset list and a realistic program plan for achieving compliance.

For More Information:
Network & Security Technologies
161 North Middletown Road
Pearl River, NY 10965
Voice: 845.620.9500
e-mail: info@netsectech.com
URL: http://www.netsectech.com

Network & Security TECHNOLOGIES