September 23, 2003

EnergyPulse™ Insight, Analysis and Commentary on the Global Power Industry

http://www.energypulse.net

NERC Compliance: Where to Begin?

Network & Security Technologies

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

The **N**orth **A**merican **E**lectric **R**eliability **C**ouncil (NERC) Urgent Action Cyber Security Standard is intended to ensure that all entities responsible for the reliability of the bulk electric systems of North America identify and protect critical cyber assets that control or could impact the reliability of the bulk electric systems. Through self-regulation, this standard requires every entity participating in North America's electricity grid to take responsibility for their Cyber Security practices. Each must verifiably do their part to ensure the security of North America's electricity and the well-being of the consumers who they serve.

The implementation plan for the NERC Cyber Security Standard states that responsible entities must examine their policies and procedures and assemble necessary documentation to meet the requirements of the standard. Through our work on NERC compliance with many energy companies we find that documentation of policy and procedure fall into three categories:

CATEGORY 1: Documented processes exist.
CATEGORY 2: Processes exist, but are not documented.
CATEGORY 3: Neither processes nor documentation exists.

Not surprisingly, among the companies surveyed we have found that the majority of NERC required processes fall into CATEGORY 2. Considering the emphasis of the NERC Standard, many will find a thorough security documentation assessment the best place to begin their compliance program.

Beginning NERC Cyber Security compliance with a policy and procedure documentation assessment has several benefits:

1. Often, cyber security problems seem intractable because of the technology, people and politics involved. A careful documentation review enables an organization to decompose the compliance program into a manageable set of prioritized tasks.
2. An objective review of existing documentation will expose the deficiencies in the organization's overall security not just in documentation, but also in processes and technologies. Although good documentation is important, good cyber security is more

important.

3. Policy and procedure cannot effectively exist without good documentation. Policy is a prerequisite for all other portions of the security program. Security procedures (e.g. disaster recovery, business continuity, monitoring, incident response, administration and maintenance) must be written to enable responsible personnel to execute them.

The NERC Cyber Security Standard specifies that the responsible entity shall **maintain** its documentation. It establishes a set of criteria for evaluating an energy company's practices through these documents. Where documentation exists, the company must evaluate whether or not the processes comply with the Standard. Then, they must determine if the documentation provides a sufficient description in an easily understood and maintained format.

The assessment of the documentation requires the company to ascertain its existence. They must evaluate its quality. In some cases, documentation may exist but is hopelessly out of date. Often, there is no process for keeping the documentation up to date. In other cases, the documentation lacks a common look and feel or overall framework that is usable by all responsible for cyber security.

Many organizations take advantage of the documentation assessment to specify this missing policy and procedure framework. Through this effort, they ensure that it is consistent, supportable, clear, concise and relevant. By taking this approach, they not only identify the gaps, but also develop a useful structure for current and future documentation.

This is where you start!

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

Network &Security TECHNOLOGIES