Challenging Requirements

In 2006, the North American Electric Reliability Council (NERC), which is responsible for the nation's Bulk Electric System, adopted permanent reliability standards for cyber security, CIP-002-1 through CIP-009-1. These standards set a high bar for the security of Cyber Assets. Responsible Entities must identify their Cyber Systems and Cyber Assets that are essential to their reliable operation. They must then implement a comprehensive set of strong procedural, electronic and physical security controls to protect those Cyber Assets against misuse as well as malicious or accidental damage.

Since the initial adoption, NERC has released, and continues to release, increasingly inclusive and stringent updates to the initial reliability standards, as well as developed new reliability standards. The bar is continually rising for the security of BES Cyber Systems and associated BES Cyber Assets.

Most organizations are likely to discover that the task of becoming fully and auditably compliant with these standards will require significant amounts of time and effort. They will often have to devote significant personnel resources just to planning their compliance projects. Simply reading, digesting, and understanding the NERC documents requires considerable attention from senior technical staff. For most Responsible Entities, the time spent on compliance will take time away from other, pressing operational matters. Moreover, few organizations possess sufficient personnel resources with experience in cyber security. Thus, drawing from existing staff does may not represent an efficient or effective means to achieving the required results.

The Energy Policy Act of 2005 creates additional urgency. NERC has become the North American Electric Reliability Corporation and is the Electric Reliability Organization reporting to the Federal Energy Regulatory Commission (FERC). While FERC is actively reviewing the NERC reliability standards, the comments of the FERC staff imply that the requirements for cyber security may become more, not less, stringent. NERC's penalties for non-compliance with reliability standards will be severe.

Where Do You Stand? How Much Work is Required?

As Responsible Entities kick off their compliance programs for new or updated Cyber Security Standards, two questions are immediately raised: "Where do we stand?" and "How much work will be needed to become compliant?" To answer these questions properly requires a detailed review of the Responsible Entity's existing processes, documentation and records. These questions need to be asked not only for control centers, but for substations, generation plants, switching stations, and other remote facilities. To even ask the right questions requires comprehensive knowledge of the standards, the technology and the industry itself.

For each of the processes, documentation and records required for compliance, Responsible Entities will need to know how much time and money is required to create NERC-compliant artifacts. This will allow a company's compliance program to be properly funded and supported. Also, since cyber security compliance is not done when the dates in the NERC Implementation Plan are met, understanding and correctly estimating the ongoing compliance burden of the CIP standards are critically important.

Voice (845) 620-9500 Fax (845) 512-2093
http://www.netsectech.com

NERC CIP COMPLIANCE ASSESSMENT

IT'S TIME TO UNDERSTAND THE NERC CYBER SECURITY STANDARDS - AND HOW FAR YOU NEED TO GO

The Expert Help You Need with Gap Analysis

N&ST has been closely following the development of all CIP reliability standards, and understands both the letter and spirit of the regulations. As an independent, product-neutral, expert consultancy, N&ST can help Responsible Entities measure the work required for compliance with the Cyber Security Standards. N&ST consultants have worked with Bulk Electric System participants to protect the cyber assets essential for the reliability of the Bulk Electric System even before Urgent Action Standard was written. These efforts have led to the creation of a simple but effective compliance assessment tool.

N&ST has a unique approach to measuring the work required for compliance with the Cyber Security Standards. N&ST's custom compliance assessment (or "gap analysis") tool helps Responsible Entities understand all of the required processes, documents and records. Where processes (including technology implementation), documents and records are missing or incomplete, N&ST estimates the work required to create or update those compliance artifacts. Each area that needs attention is prioritized based on the dates in NERC's Implementation Plan, the work required for compliance, and dependencies in the compliance program. Finally, N&ST estimates the on-going effort required to maintain compliance with the Cyber Security Standards. All of these detailed findings are summa-rized in an Executive Report and an Executive Presentation. This report and presentation will help justify funding for the Responsible Entity's compliance program for the Cyber Security Standards.

Once the gap analysis is complete, the Responsible Entity is left with a tool for organizing and prioritizing their remediation program. Working independently or with help from N&ST, the Responsible Entity can create a detailed remediation plan for compliance by the dates in NERC's Implementation Plan. Then, the Responsible Entity can track their progress towards addressing the deficiencies identified during the gap analysis. N&ST's compli-ance tool includes a detailed list of every process, document and record required to demonstrate full compliance with the all Cyber Security Standards.

N&ST has experience assessing all types of Cyber Systems and Cyber Assets. N&ST expert consultants have visited some of the nation's largest generating facilities and substations to prepare those facilities for compliance with the NERC Cyber Security Standards. Understanding how the CIP standards apply to these environments and how to build appropriate security perimeters is essential to efficiently estimating the work required for a comprehensive NERC CIP compliance program.

On-time and On-budget

N&ST prides itself on delivering its projects on-time and on-budget using skilled resources. All N&ST consultants are full-time employees with many years of computer networking, cyber security, and electric utility industry experience. Our projects are care-fully managed to ensure complete client satisfaction within the quoted time frame and price. As a product- neutral vendor, N&ST is not simply trying to solve client problems using a specific device or product. Instead, N&ST is focused on delivering practical and innovative solutions to our clients most challenging compliance problems!

N&ST WILL HELP YOU MEASURE THE WORK REQUIRED TO ATTAIN COMPLIANCE

Network &Security Technologies

Our passion for technical excellence and commitment to our client's business success results in practical solutions to complex problems

161 North Middletown Road, Pearl River, NY. 10965