The Gap Analysis Is Done – Now the Real Work Begins

Network & Security Technologies, Inc. (N&ST) has a complete portfolio of services designed to help Bulk Electric System participants comply with the cyber security requirements in NERC CIP-002 through CIP-009. An important initial step on the road to compliance for any Responsible Entity is a gap analysis. That undertaking, which N&ST has performed for multiple Responsible Entities, provides a point in time view of how well a client's existing security processes, documents, and records satisfy the CIP requirements, and identifies what gaps must be addressed.

The NERC CIP Standards define where Responsible Entities must be in terms of cyber security processes, documentation, and records in order to be fully compliant. Once a gap analysis has been completed, a Responsible Entity will have an answer to the question, "Where are we now?" Depending on the scope of the analysis, a basic set of required gap remediation tasks may have been identified, along with order-of-magnitude cost estimates. However, in most instances, the critical questions, "How do we get to where we need to be?" and, "How do we get there on time?" will have been answered at only a very high level. N&ST has the expertise and experience necessary to assist Responsible Entities with both the planning and execution phases of their gap remediation projects.

The Expert Help You Need with Compliance

The specific task and schedule requirements of a Responsible Entity's remediation project will, of course, depend on factors including the size and complexity of their information technology infrastructure and the results of their most recent CIP Standards gap analysis. N&ST works closely with each individual client to define a set of tasks that is appropriate to the client's specific needs. A comprehensive remediation project typically includes several or all of the following representative tasks:

Critical Asset and Critical Cyber Asset Identification

N&ST can work with Responsible Entities to properly identify and document their Critical Assets (generation units, control centers, substations, etc.) and associated Critical Cyber Assets. N&ST has developed documentation templates for the risk-based assessment methodology and asset lists required by NERC and will help Responsible Entities prepare these documents. In many cases, not all Cyber Assets associated with a Critical Asset should be considered Critical Cyber Assets. Because of N&ST's deep experience with TCP/IP networks and control system components, N&ST's expert consultants can help Responsible Entities ensure that the correct Cyber Assets are listed as Critical Cyber Assets.

Cyber Security Policy Development

N&ST's experience with Bulk Electric System customers suggests that while most Responsible Entities have at least high-level cyber security policies, nearly all of them will have to update their policies to address the specific requirements of CIP-002 through CIP-009 as required by CIP-003. N&ST consultants can draw on experience with developing policies for compliance with an array of standards, including ISO 17799, HIPAA, and PCI, and combine it with our CIP Standard expertise to create these important artifacts of CIP Standard compliance.

...CONTINUED ON NEXT PAGE

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

NERC CIP GAP REMEDIATION

Security Perimeter Design

In many instances, there may be more than one way to define CIP-compliant Electronic and Physical Security Perimeters around a given set of Critical Cyber Assets. The approach chosen can have a significant impact on the costs to either achieve or maintain compliance. For example, moving non-critical Cyber Assets outside of a proposed Electronic Security Perimeter (ESP) could require a major network redesign and compel the acquisition of new networking equipment, such as firewalls and filtering routers, to create required electronic access points. However, a decision to leave non-critical Cyber Assets within an Electronic Security Perimeter could result in even higher ongoing costs due to the fact that all Cyber Assets inside an ESP, both critical and non-critical, are subject to the extensive requirements of CIP-007 ("Cyber Security — Systems Security Management"). Similarly, the manner in which Electronic Security Perimeters are defined can impact a Responsible Entity's requirements for Physical Security Perimeters.

N&ST can help Responsible Entities to define candidate security perimeter configurations and to identify and evaluate the cost/benefit trade-offs among the candidates. Once solutions that best fit a particular client's environment, budget, and capabilities have been selected, N&ST can assist with required CIP-005 and CIP-006 documentation using standardized templates

Access Control Design

An important second-order task following Electronic Security Perimeter definition is designing and implementing access control mechanisms for electronic access points. Responsible Entities must comply with the CIP-005 requirement to deny access by default and allow only explicitly permitted traffic to transit Electronic Security Perimeter access points. N&ST consultants can apply experience gained from nearly two decades of designing, configuring, evaluating and optimizing Internet and intranet firewalls for Government and commercial clients to help Responsible Entities ensure that the data traffic crossing their Electronic Security Perimeter boundaries is necessary, originates from the right sources, and is being sent to the right destinations.

System Security

N&ST can apply its expertise with computer system hardening in Windows, Unix, and Linux environments to help Responsible Entities address the CIP-007 requirements for Ports and Services, Security Patch Management, and Malicious Software Prevention for all Cyber Assets within Electronic Security Perimeters. N&ST also understand how to apply the CIP standards to purpose-built electric utility industry equipment such as relays, RTUs, plant control systems and PLCs.

Expert consultants from N&ST also have years of experience conducting vulnerability assessments on and within ESPs without disturbing the operation of critical systems.

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 carefully managed to ensure complete client satisfaction within the quoted timeframe 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!

Network &Security Technologies
161 North Middletown Road, Pearl River, NY. 10965

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