

NERC CIP CYBER VULNERABILITY ASSESSMENT

A Critical Environment Needs an Innovative Approach

The NERC Critical Infrastructure Protection (CIP) standards require routine cyber security vulnerability assessments. These must identify flaws or weaknesses in protective measures while avoiding the introduction of additional risk to essential systems. In this way, CIP-005 Requirement R4 and CIP-007 Requirement R8 can be likened to non-destructive structural testing methods employed by bridge and building inspectors. The challenge is to find potential problems without resorting to traditional penetration testing tools that can impair the networks and computers that make up energy management systems (EMS). Network & Security Technologies (N&ST) has developed just such an approach. Based on years of helping electric power customers achieve NERC CIP compliance, our methodology does not require risky connection of test equipment to sensitive networks or the deployment of unsupported software.

Achieve the Requirements

The most important goal for any NERC CIP vulnerability assessment is to satisfy the minimum requirements of CIP-005 R4 and CIP-007 R8, namely:

- Discover all access points to the electronic security perimeter (ESP),
- Verify enabled ports and services at each access point,
- Review controls for default accounts, passwords, and network management community strings for each ESP access point.
- Verify that only ports and services required for normal or emergency operations are enabled on each system, and
- Review the controls for default accounts for each system.

These simple objectives demand considerably more effort and expertise than many people expect. Moreover, these requirements don't just apply to an organization's critical cyber assets (CCA) and cyber assets within the ESP. They must address the systems that control and monitor both the ESPs and physical security perimeters (PSP) that protect them.

How We Work in Your Complex Environment

N&ST consultants have the expertise to perform the CIP vulnerability assessment:

- Technical knowledge of EMS and SCADA environments used by the industry,
- Detailed understanding of the communications protocols running in control system networks,
- Knowledge of a wide variety of network devices, servers, workstations, operating systems, and application software,
- Knowledge of RTUs, relays, IEDs, and telecommunications equipment used in substations and generation plants,
- Hands-on experience configuring ESP access points and reviewing their access control lists,
- Full command of the NERC CIP standards, and
- Strong writing and documentation skills.

In addition, all N&ST personnel have a clear background checks satisfying the personnel risk assessment requirements of CIP-004.

Our Standard, Proven Methodology

Every engagement begins with a survey of existing data sources. Where possible, the team will utilize your existing records and listings from CIP compliance and support activities. Often, this information will suffice for many or even most of the sub-requirements. When the consultants do need more data, they know how to get it without modifying software or equipment configurations. Instead, they work with support staff to use native reporting and diagnostic functions available in most EMS, SCADA, and network devices to generate the requisite records and lists. These can serve other purposes as well. For example, responsible entities can use some of the lists to demonstrate compliance with CIP-007 requirement R2, Ports and Services.

As a final check on the raw data, N&ST will perform a physical walk-through of the facilities that house the cyber assets. They will verify the locations of the cyber assets, cabling, and other aspects of the equipment layouts.

N&ST will then perform numerous analyses and reviews. For example, they will:

- Verify schematics,
- Review access point configurations,
- Analyze network IP addresses and subnet masks,
- Examine accounts lists and control procedures, and
- Review records of password and configuration changes.

Finally, the consultants will document their observations, findings, and recommended remediation or mitigation activities.

Work Smart, Get Results, Save Time

N&ST has the know-how to meet your NERC CIP vulnerability assessment needs. Our team has developed a repeatable methodology that satisfies the cyber security standard requirements without increasing risk to your reliability operations. We have hands on experience with most North American Energy Management Systems (EMS) as well as a wide variety of RTUs, relays, IEDs, and network devices used for substations and generation plants, so we won't waste time learning about your hardware or software.

Our approach enables you to have the information you need to protect against threats introduced through "feature creep," account modifications, and other security vulnerabilities introduced over time. We can enhance our basic service offering to verify other aspects of your electronic and physical security plans, for example patch levels and malicious software prevention. Most importantly, we work quickly and efficiently so that you can meet your compliance deadlines and avoid negative audit findings.