Network &Security Technologies

NERC CIP RSAW PREPARATION

NERC CIP RSAW PREPARATION

Time for an Audit

As part of the Bulk Electric System (BES), your organization can expect an audit against the North North American Electric Reliability Corporation (NERC) cyber security standards CIP-002 through CIP-011 and CIP-014. This will include a review of artifacts – documents and records – as well as implemented measures – technology, organizational processes, and procedures. NERC has developed a series of Reliability Standard Audit Worksheets (RSAWs) to guide and track the process. These provide a uniform template for identifying and evaluating compliance evidence. They include fields for completion by your subject matter experts prior to a site visit by auditors or an off-site review of evidence. Ideally, the responses will supply all the information required by the audit team to locate, understand, and evaluate the CIP security measures.

Are You Ready?

Completion of the RSAWs demands more effort than many might expect. While the audit team will request immediate access to process documents and records, they usually won't do any legwork or digging work looking for details that they may require. It's the job of the responsible entity to pull it all together gather the correct information. The worksheets provide a logical order for organizing artifacts and a formal method for communication between you and the compliance enforcement authority. Because some of the 100+ CIP requirements do not specify documentation or records; your organization must describe and substantiate your compliance measures within the worksheet alone. For this reason, many companies will find that "full compliance" differs from "verifiable compliance."

Network & Security Technologies (N&ST) has already supported several BES companies with completing RSAWs and preparing for a NERC CIP audit. N&ST has also acted as a Regional Entity auditor and reviewed many completed RSAWs. We have worked with the cyber security standards since their inception, in 2006. Our consultants know what to expect and how to phrase responses to auditors. As a neutral party, N&ST can objectively judge the quality of compliance evidence.

Get a Head Start

Our engagements begin with a brief survey of the current CIP program. We meet with your people to learn about the location of documents and records. Since the goal is to catalog compliance measures rather than evaluate them, our consultants can usually perform this phase without disrupting your team's normal activities. Instead, they gather the CIP artifacts for later analysis.

Following the survey, N&ST will work requirement-by-requirement. We will read your cyber security documentation and review records to determine the specific citations that respond to the standard. For each RSAW section, we compose appropriate language to guide auditors to the specific evidence they seek. Often, our consultants recommend and devise common naming conventions and documentation formats to ensure all data are readily accessible.

In those cases where no documentation exists, N&ST meets with appropriate subject-matter experts to determine what your organization does to conform to the CIP requirement. We draft appropriate descriptive language for the RSAW section. Then, our consultants collaborate and finalize the response with the experts. If we find a missing measure, we recommend an appropriate solution for your organization. We can even help with it's implementation.

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

NERC CIP RSAW PREPARATION

RESPONSIBLE ENTITIES WILL REQUIRE MORE THAN JUST THE APPROPRIATE COMPLIANCE EVIDENCE AND ARTIFACTS

The TFE

Sometimes a technical feasibility concern prevents full compliance with a particular CIP measure. In these cases, we review the existing technical feasibility exception (TFE) to ensure it is complete and correct. We then include a citation to the TFE documentation within the RSAW response. If, for some reason, an exception is required but not yet filed, N&ST provides the expertise to put one in place that meets all the provisions of the NERC process.

On-time and On-budget

N&ST prides itself on delivering its projects on-time and on-budget using skilled resources. We have the know-how to meet your NERC CIP needs. Our consultants will follow a repeatable methodology to identify compliance gaps and recommend remediation. We won't waste time because we:

- Participate in NERC CIP Standards Drafting Team meetings
- Know the current CIP-002 through CIP-011 and CIP-014 requirements
- Work with many BES companies across all aspects of the industry –
- transmission, generation, distribution, balancing and reliability coordination, etc.
- Understand most Energy Management Systems (EMS)
- Have hands-on experience with SCADA technologies including many RTUs,
- relays, IEDs, and telecommunications
- Understand routable protocols and data networks
- Support numerous CIP RSAW and compliance analysis
- projects Serve on NERC and Regional Entity CIP audit teams

Our approach enables you to have the information you need to protect against cyber security threats. Most importantly, we work quickly and efficiently so that you can meet your compliance deadlines and avoid negative audit findings. All N&ST consultants are full-time employees with many years of computer networking, cyber security, and electric utility industry experience. We carefully manage our projects to ensure complete customer satisfaction within the quoted time frame and price.

THE RELIABILITY STANDARD AUDIT WORKSHEET (RSAW)

- Provides a uniform methodology to identify and evaluate compliance evidence,
- Requires input from the responsible entity (you), and
- Establishes a formal and objective communication channel between you and the audit team.

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