

## NERC CIP Mock Audit

### Are You Prepared for Your NERC CIP Audit?



The approval of the NERC (North American Electric Reliability Corporation) cyber security standards (CIP-002 through CIP-009) has changed the status quo for Bulk Electric System (BES) companies like yours. They have transitioned informal cyber protection schemes to a complex program of technical and procedural security measures. Now, with the definition of the electric power ERO (Energy Reliability Organization) and the assignment of its function to NERC, these standards have the effect of law. Failure to implement them correctly will result in significant financial sanctions.

Moreover, public release of negative findings by a CIP auditor can have dire consequences in terms of reputation, customer confidence, and the ability to conduct business.

Responsible Entities have worked diligently to meet the compliance deadlines laid out in the NERC CIP Implementation Plan. They've modified their organizations, written policy, developed procedures, and have begun detailed record-keeping activities to achieve the milestones for each of the 41 individual requirements found in the standards. Most must be "Auditably Compliant (AC)" some time in 2010. This means "...the entity meets the full intent of the requirement and can demonstrate compliance to an auditor, including 12-calendar-months of auditable "data," "documents," "documentation," "logs," and "records." NERC intends to meet these goals through an aggressive CIP auditing program.

### Confidence Comes Only with Practice

For the most part, compliance programs have focused on putting the necessary technologies, processes, and procedures in place. They've involved the acquisition of hardware and software as well as document writing; affecting a wide segment of most organizations. Some larger entities must address needs such as training and personnel risk assessments of more than a thousand individuals – including employees and contractors.

#### Will I Pass the NERC CIP Audit?

- Proving compliance is more than just implementing security measures
- Auditors will expect entities to quickly produce their "data," "documents," "documentation," "logs," and "records"
- Some IT support personnel may lack experience in dealing with a rigorous audit team

**Our Mock Audit will enable you to understand what to do beforehand to avoid negative audit findings**

The NERC audit timeline will not afford investigators much leeway to explore your organization's unique set of security measures. Instead, they will expect you to produce all evidence in a clear and concise form. Moreover, each artifact must be ready for inspection when the audit team arrives. They will have little tolerance for delays and even less for incomplete documents or records. Materials that are missing during the visit will result in a negative finding, even if your organization has substantially addressed the CIP requirements.

Now that the implementation phase for CIP compliance is reaching a close, many managers like you are unsure that their organization's work will stand up to the rigorous scrutiny of the auditor's microscope. Their team spent long hours putting myriad security measures into place by focusing on functional issues. Considerably less time was taken to make the work presentable. Even if their activities were well organized, few have considered how it

**The most important CIP implementation milestone is "Auditably Compliant."**

**Our "in the room" experience enables us to simulate the environment and atmosphere that entity personnel are likely to face during a real NERC CIP audit.**

Our passion for  
Technical excellence  
and commitment to  
our clients' business  
success results in  
practical solutions  
to complex  
problems

**Contact Us:**

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

**Phone:**  
(845) 620-9500

**Fax:**  
(845) 512-2093

**E-mail:**  
[info@netsectech.com](mailto:info@netsectech.com)

**URL:**  
[www.netsectech.com](http://www.netsectech.com)

will look to an auditor.

Like many others, you may want to put your compliance program to the test. You can do this by conducting an internal mock audit in advance of any visit by NERC. This simulates the experience your organization will face once the Auditably Compliant deadlines have passed and a real CIP-002-1 through CIP-009-1 audit is scheduled. In so doing, you can make necessary adjustments to reduce significantly the likelihood of negative findings. Moreover, your cyber security team will have the chance to see their work through the eyes of an objective and critical examination.

### ***The Mock Audit – A Dress Rehearsal***

Network & Security Technologies, Inc. (N&ST) has developed the Mock Audit to enable you to understand how well your CIP compliance program will stand up to scrutiny by NERC auditors. Our consultants have spent time on both sides of this process – they have served as subject matter experts on the examination team as well as supported companies during a review. This “in the room” experience enables us to simulate the environment and atmosphere that your CIP compliance team will face.

The N&ST service offering examines all aspects of your organization's compliance program in the same way that an audit team will. They review documents, processes, procedures, records, and other evidence of compliance within the time constraints afforded a real team. They will follow the same rules used by trained NERC investigators when interviewing your people, such as “trust but verify”. Most importantly, they will address the process with the objectivity and detachment that a real audit team will use.

The deliverable will identify the findings you can expect to see along with an explanation of what gaps exist. For example:

- A document does not have required data, such as full names and dates.
- One or more records appear to have missing entries.
- Information such as a date in one artifact contradicts that of another.
- An individual lacking an up-to-date personnel risk assessment or training accessed a critical cyber asset.
- The implemented measure does not address the corresponding CIP requirement.
- Requested artifacts were not presented within the time allotted.
- The interviewed subject matter expert lacked knowledge or credibility.

At the end of the N&ST CIP Mock Audit, your company will have a report that provides it with actionable recommendations to improve your processes and increase the probability that your NERC CIP audit will result in zero negative findings. Moreover, you will have access to industry leaders with experience implementing all 41 of the requirements called for by the standards. This will give you the confidence to face any investigation of your organization's cyber security program.

