NERC CIP Critical Asset Assessments

NERC CIP CRITICAL ASSETS

The question facing most companies preparing for NERC CIP standards compliance is “where do we start?” With eight individual CIP standards each with their own numerous requirements, how to start is a fair question.

- Electronic Security (CIP-002, CIP-003, CIP-005, CIP-007, CIP009)
- Physical Security (CIP-006)
- Personnel, Training & Management (CIP-004, CIP-008)

The most logical starting point is with a facilities-wide assessment addressing the requirements outlined in NERC CIP-002 Critical Cyber Asset Identification. Trying to directly implement a hardware or software solution without first complying with CIP-002 will ultimately cost you more money as you may buy a solution that is way over scope and protect assets that are not deemed critical. Or worse, risk paying significant fines and penalties for lack of compliance, ranging as high as $1 Million dollars per day.

WHAT ARE NERC CIP CRITICAL ASSET?

The CIP-002 standard outlines definitions and a methodology to be used in defining Critical Assets (CA) and Critical Cyber Assets (CCA). NERC Standard CIP-002 R3 requires that each facility develop a list of CCAs that are essential to the operation of its CA.

The NERC CIP definition for Critical Assets (CA):

“Facilities, systems, and equipment which, if destroyed, degraded, or otherwise rendered unavailable, would affect the reliability or operability of the Bulk Electric System.”

The NERC CIP definition for Critical Cyber Assets (CCA):

“Cyber Assets essential to the reliable operation of Critical Assets.”

The first phase taken to comply with CIP-002 needs to be a comprehensive risk-based assessment. The following steps should be taken to ensure that all critical assets are identified.
Operational Risk Assessment:
A list of all critical operational assets are identified. This would include assets such as control environmental, alarms, safety and continuous power.

Network Vulnerability Assessment:
A network vulnerability is performed to accurately depict the current security posture of cyber assets associated with critical infrastructure.

Gap Analysis:
A comprehensive risk assessment will identify and outline gaps to be reviewed. A gap analysis should be performed to evaluate current practices in accordance with policies and CIP requirements.

Security Awareness and Policy Review:
A general review of all policy documents and operational security awareness should be performed to assess the overall effectiveness in accordance with CIP requirements.

The CIP-002 R3 standard further qualifies Critical Cyber Assets (CCA) as those assets that meet any of the following qualifying connectivity requirements:

R3.1. The Cyber Asset uses a routable protocol to communicate outside the Electronic Security Perimeter
R3.2. The Cyber Asset uses a routable protocol within a Control Center
R3.3. The Cyber Asset is dial-up accessible

This table is an example of how a facility might apply these standard in determining if an identified asset is a Critical Cyber Asset (CCA)

<table>
<thead>
<tr>
<th>Cyber Asset</th>
<th>R3.1</th>
<th>R3.2</th>
<th>R3.3</th>
<th>Communication</th>
<th>Critical Cyber Asset (CCA)</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;Entity Identifier&gt;</td>
<td>Y</td>
<td>N</td>
<td>N</td>
<td>Routable IP</td>
<td>Y</td>
</tr>
<tr>
<td>&lt;Entity Identifier&gt;</td>
<td>N</td>
<td>N</td>
<td>Y</td>
<td>Dial-up</td>
<td>Y</td>
</tr>
<tr>
<td>&lt;Entity Identifier&gt;</td>
<td>N</td>
<td>N</td>
<td>N</td>
<td>Serial</td>
<td>N</td>
</tr>
</tbody>
</table>

HOW CAN THE INVENSYS CYBER SECURITY TEAM HELP?

Understanding the NERC CIP regulations in their entirety is a large task. Having the expertise and ability to execute an effective assessment plan and then launch a comprehensive remediation program can seem virtually impossible. This is where the Invensys Critical Infrastructure and Security team can help. Invensys not only has the expertise and knowledge to help your facility become NERC-CIP compliant, but we also understand that effective Cyber Security is a lifetime program. To manage this commitment, Invensys has developed a Cyber Security Lifecycle approach that can be applied at any stage, from an initial Assessment to Architecture and Policy Development as well as Modernization and Implementation right through to Security Management and Optimization.

To learn more about Invensys’ Cyber Security Lifecycle portfolio, contact your sales representative or visit: http://iom.invensys.com/CyberSecurity.