NERC CIP Gap Analysis – How to Get Started

June 2006
Agenda

• Introduction
• What should I know before starting?
• What do I need?
• What should I expect from the analysis?
• How much time will it take?
• Conclusions and questions
Introduction

Nick Lauriat

Principal Architect

161 North Middletown Road   Pearl River, NY 10965
mobile: 781.572.1400   fax: 845.620.1526
e-mail: nlauriat@netsectech.com
URL: http://www.netsectech.com
Agenda

• Introduction
• **What should I know before starting?**
• What do I need?
• What should I expect from the analysis?
• How much time will it take?
• Conclusions and questions
NERC CIP Standards

Permanent Cyber Security Standards

CIP-002-1 Critical Cyber Assets
CIP-003-1 Security Management Controls
CIP-004-1 Personnel and Training
CIP-005-1 Electronic Security
CIP-006-1 Physical Security
CIP-007-1 Systems Security Management
CIP-008-1 Incident Reporting and Response Planning
CIP-009-1 Recovery Plans
Review the Standards

• Don’t rely on others—take the time yourself.

• Focus on the Requirements and Measures.
  – These are the “meat.”
  – Other language is only meaningful in context.

• At least know the 8 categories for CIP-002-1 through CIP-009-1
# NERC Implementation Plan

<table>
<thead>
<tr>
<th>PHASE</th>
<th>DEFINITION</th>
</tr>
</thead>
<tbody>
<tr>
<td>Begin Work (BW)</td>
<td>A Responsible Entity has developed and approved a plan to address the requirements of a standard, has begun to identify and plan for necessary resources, and has begun implementing the requirements.</td>
</tr>
<tr>
<td>Substantially Compliant (SC)</td>
<td>An entity is well along in its implementation to becoming compliant with a requirement, but is not yet fully compliant.</td>
</tr>
<tr>
<td>Compliant (C)</td>
<td>The entity meets the full intent of the requirements and is beginning to maintain required “data,” “documents,” “documentation,” “logs,” and “records.”</td>
</tr>
<tr>
<td>Auditably Compliant (AC)</td>
<td>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.”</td>
</tr>
</tbody>
</table>
Understand How the Plan Applies to You

• Determine the NERC Entity type(s) that apply to your organization.
  - Balancing Authority
  - Transmission Operator
  - Reliability Coordinator
  - Transmission Service Provider
  - Regional Reliability Organization
  - Interchange Authority
  - Transmission Owner
  - Generator Owner
  - Generator Operator
  - Load Serving Entity

• Understand what role your organization plays in the “Bulk Electric System.”
Agenda

• Introduction
• What should I know before starting?
• **What do I need?**
• What should I expect from the analysis?
• How much time will it take?
• Conclusions and questions
Identify a Team

- Include knowledgeable personnel:
  - Operations
  - Support
  - IT
  - Telecommunications
  - Human Resources
  - Facilities
  - Physical Security
  - Information Security
  - Audit

- This team will vary from company to company depending upon what type of role they play in the market and organizational structure.
Get Help

- Few companies have personnel who can read and interpret all the CIP standards.
- Try to find external expertise with experience in the industry – not generic IT security assessments.
- Collaborate with consultants, don’t go for the stand-alone “assessment report” approach.
- Take the opportunity to bring staff up to speed.
- Use NERC and NPCC resources.
Start With What You’ve Got

• **Documents:**
  - Collect all procedural and technology descriptions.
  - Identify handwritten notes or emails – these are documentation, just not formal.

• **Review other security assessments.**
  - Don’t reinvent the wheel.
  - Don’t duplicate the efforts of others.

• **Work with audit groups.**
  - They often have very useful insights.
  - Mine other types of assessments and audits.
Identify Critical Assets

• Define “risk based” criteria.
• Create a list of assets that meet them:
  – Control Centers
  – Generation Facilities
  – Substations
  – Other Assets
Identify Critical Cyber Assets

• Are there Critical Cyber Assets at the plant or substation?

• **IF** nothing meets these criteria:
  – The Cyber Asset uses a routable protocol to communicate outside the Electronic Security Perimeter; or,
  – The Cyber Asset uses a routable protocol within a Control Center; or,
  – The Cyber Asset is dial-up accessible.

• **THEN** you have no Critical Cyber Assets!  Stop!
Think About Interpretation

• How do the standards apply to your environment? For example:
  – Who’s in charge right now?
  – Who should be in charge?
  – What policy exists right now?
  – Are your substations networked?
  – Has your power plant control system been upgraded?
  – What physical and electronic perimeters are defined today?

• These questions will lead to your own interpretation.
Identify a “Goal State”

• Your interpretation is how the standards apply to your environment.
  – A “goal state” is where you need to be for compliance.
• Write down your interpretation.
• Perform your gap analysis against this written interpretation, not someone else’s.
Agenda

- Introduction
- What should I know before starting?
- What do I need?
- **What should I expect from the analysis?**
- How much time will it take?
- Conclusions and questions
Set Near-Term Goals

- The first gap analysis should enable you to “Begin Work.”
- You should get *projects* and *tasking*.
- Technology specifications, policies, procedures, and other issues will come later.
- The compliance program evolves over time, so we don’t want too much detail now.
Focus on Compliance

• Avoid “piling on” a comprehensive security assessment because this is a “good opportunity.”

• Insist that findings tie directly to specific CIP requirements, not general “best practice.”

• Prioritize based on magnitude of compliance liability.
Don’t Obsess

• Eschew detailed “score sheets” in favor of direct findings.
  – Priorities: High and Low, not 1 to 10
  – Costs: Rough order of magnitude, not precise $
  – Time: Answer the question, “How many resources will I need for how long?” not hours and minutes for each task.

• We want to point the way to achieving compliance, not define the discrete tasks for the entire program.
Analysis Tracks Asset Types

- Control Centers
- Generation Plants
- Substations
Control Centers

- Sophisticated IT environment
- A single, contiguous physical security perimeter (generally)
- Central control of electronic access and system management
- Small, well-trained support team
- Potential experience with NERC Urgent Action Cyber Security Standard 1200
Generation Plants

- Disjoint IT environment with little central control
- Difficult to define physical security perimeter
- Few, if any, electronic access controls or system management
- Untrained personnel with little centralized support (at least in terms of security)
- No experience with NERC 1200
Substations

- Varied and inconsistent IT environment (some fully automated, some exclusively electromechanical)
- Well defined physical security perimeter (station house)
- Electronic access often uncontrolled
  - Dial modems or wide open routable networks
- Inconsistent system management
  - Substations are often built and maintained by committee!
- Untrained personnel with diverse backgrounds and legitimate reasons for entering the house
- No experience with NERC 1200
- Things could be changing – fast!
Agenda

• Introduction
• What should I know before starting?
• What do I need?
• What should I expect from the analysis?
• **How much time will it take?**
• Conclusions and questions
How Much Time Will It Take?

• Depends upon:
  - The depth of review
  - The size of the organization
  - The types and number of assets
  - The current compliance level

• An initial gap analysis will take longer than a follow-up gap analysis.
## Rough Estimates

<table>
<thead>
<tr>
<th>Phase</th>
<th>Initial Analysis</th>
<th>Second Analysis</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Kick-off</strong></td>
<td>1 – 3 days</td>
<td>1 day</td>
</tr>
<tr>
<td><strong>Data Gathering</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>– Enterprise-wide</td>
<td>5 – 10 days</td>
<td>2 – 5 days</td>
</tr>
<tr>
<td>– Control Center</td>
<td>10 – 15 days</td>
<td>5 – 10 days</td>
</tr>
<tr>
<td>– Plants</td>
<td>1 – 3 days each</td>
<td>½ to 1 day each</td>
</tr>
<tr>
<td>– Substations</td>
<td>1 – 2 days each</td>
<td>¼ to ½ day each</td>
</tr>
<tr>
<td><strong>Analysis</strong></td>
<td>1 – 3 times data</td>
<td>1 – 3 times data</td>
</tr>
<tr>
<td><strong>Reporting</strong></td>
<td>2 – 10 days</td>
<td>1 – 5 days</td>
</tr>
</tbody>
</table>
Agenda

- Introduction
- What should I know before starting?
- What do I need?
- What should I expect from the analysis?
- How much time will it take?
- Conclusions and questions
Conclusions

• Do your homework:
  – Understand the NERC Standards.
  – Understand your organization.
• Know what you want/need.
• Budget and allocate personnel.
• Stay focused – compliance is the goal.
Thank You