Cyber Security Compliance
“Executive Call for Implementation”

Northeast Power Coordinating Council
Task Force on Infrastructure Security & Technology’s
Cyber Security Workshop
June 7 & 8, 2006

William E. McEvoy
NU Cyber Security Program Manager
Today’s Presentation

• Brief Corporate Overview

• Corporate Compliance Program

• Cyber Security Compliance Program

• Summary
Corporate Overview

Core Business
- Regulated Electric (T&D) and Gas (CT)
- Selling off all Competitive Business by end of 2006

Sales of Electricity
- Regulated Retail - 36, 200 kWh-millions

2005 Regulated Business Earnings
- $163.4 million

Customers
- 1.8M Electric and 194,200 Gas

System Territories and Footprint
- CL&P: 4,400 Square Miles, 149 Communities in CT
- WMECO: 1,500 Square Miles, 59 Communities in MA
- PSNH: 5,445 Square Miles, 211 Communities in NH

System Voltages
- 345kv, 115kv, 69kv, 34.5kv
Corporate Overview

• **Member of ISO-NE**

• **Member of NPCC**

• **Current NERC Functional Model Registration**
  – *Transmission Owner*
  – *Transmission Operator*
Corporate Compliance Program

Northeast Utilities “View on Compliance”
### Why Is Reliability Compliance Becoming Increasingly More Important?

<table>
<thead>
<tr>
<th>The Past</th>
<th>What’s Changing</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>No federal Law</strong>&lt;br&gt;No FERC involvement</td>
<td><strong>EPAct 2005 resulted in heightened accountability for system reliability</strong>&lt;br&gt;FERC oversight of all reliability standards and enforcement</td>
</tr>
<tr>
<td><strong>A weak NERC</strong>&lt;br&gt;Voluntary standards</td>
<td><strong>A strong “Electric Reliability Organization” (ERO)</strong>&lt;br&gt;Likely to be NERC&lt;br&gt;Drives and enforces approved reliability standards</td>
</tr>
<tr>
<td><strong>Ten regional councils</strong>&lt;br&gt;Standards vary between regions</td>
<td><strong>Regional Councils with enforcement authority</strong>&lt;br&gt;Likely to be similar to today; some are merging&lt;br&gt;Effort to align regional standards</td>
</tr>
<tr>
<td><strong>Voluntary commitment to standards</strong></td>
<td><strong>Must be audibly compliant with standards or face penalties</strong></td>
</tr>
<tr>
<td><strong>Voluntary commitment to standards</strong></td>
<td><strong>Must be audibly compliant with standards or face penalties</strong></td>
</tr>
</tbody>
</table>

* RFC ReliabilityFirst, is the successor organization of MAIN, ECAR, and MAAC
NERC’s Perspective: The Climb To Really Excellent Reliability Standards

Camp ‘Version 0’
**Specifically, What Is Changing?**

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>National Standards</strong></td>
<td>NERC - Voluntary* 90 revised stds</td>
<td>NERC - Voluntary version 0 adopted</td>
<td>ERO - Mandatory version 0, version 1+</td>
</tr>
<tr>
<td><strong>Registration</strong></td>
<td>6 types</td>
<td>Moving to 15</td>
<td>Held to requirements of the 15</td>
</tr>
<tr>
<td><strong>Vegetation Mgmt</strong></td>
<td>Version 0</td>
<td>Version 1 (filing requirement)</td>
<td>Auditably compliant '07</td>
</tr>
<tr>
<td><strong>Cyber Security</strong></td>
<td>1 standard</td>
<td>Standard adopted</td>
<td>Auditably compliant '09</td>
</tr>
<tr>
<td><strong>Regional Entity</strong></td>
<td>NPCC</td>
<td>NPCC</td>
<td>Cross Border Regional Entity (CBRE)</td>
</tr>
<tr>
<td><strong>Investigations</strong></td>
<td>Regional Entity</td>
<td>Regional Entity</td>
<td>Regional Entity reports violations to NERC and FERC</td>
</tr>
<tr>
<td><strong>Penalties</strong></td>
<td>All violations equal penalties simulated</td>
<td>All violations equal penalties simulated</td>
<td>Penalties with sanction guidelines</td>
</tr>
<tr>
<td><strong>RTO/ISO</strong></td>
<td>Enforcement Power</td>
<td>Enforcement Power</td>
<td>Loses enforcement power; may serve as technical expert to Cross Border Regional Entity</td>
</tr>
<tr>
<td><strong>Funding</strong></td>
<td>NPCC members charged with percentage rolling up to NERC</td>
<td>NPCC members charged with percentage rolling up</td>
<td>Load-Serving Entity (LSE) surcharge to load; ERO controls funding</td>
</tr>
<tr>
<td><strong>Regional Standards</strong></td>
<td>Guidelines/Criteria/Procedures</td>
<td>Guidelines/Criteria/Procedures</td>
<td>Mandatory Cross Border Regional Entity standards</td>
</tr>
<tr>
<td><strong>Readiness Audit</strong></td>
<td>Industry Volunteers</td>
<td>Industry Volunteers</td>
<td>Industry Volunteers</td>
</tr>
<tr>
<td><strong>Compliance Audits</strong></td>
<td>Industry Volunteers</td>
<td>Industry Volunteers</td>
<td>Cross Border Regional Entity Compliance Staff</td>
</tr>
<tr>
<td><strong>Enforcement Structure</strong></td>
<td>Modeled after self-regulating organizations (Securities Exchange Commission)</td>
<td>Same</td>
<td>Same structure, but with sanctions and penalties</td>
</tr>
</tbody>
</table>

*NERC Functional model was created in 2002, where the Transmission Operator function was defined. Prior to, there were very limited standards.*
The Time Line for Implementing Mandatory Reliability Standards

**FERC Actions:**
- FERC issued an ERO Notice of Proposed Rule-Making
- FERC issued its ERO Order
- Committee Hearing on Electricity Reliability Portion of EPAct
- FERC approves NERC Application with Compliance Directives (estimated date)
- FERC issues Reliability Standards NOPR
- FERC approves Reliability Standards
- ERO standards become effective (6-month phase-in before penalties)
- Penalties for Violations Begin

**NERC related actions:**
- NERC applies to become the ERO and petitions FERC to accept reliability standards.
- Motion to Intervene on NERC Application Filing due to FERC
- NERC-proposed Reliability Standards NOPR - comments due (estimated date)
- NERC and Regional Entities sign Regional Delegation Agreements
- NERC continues to develop new standards

Congress passes the Energy Policy Act

2005

2006

2007
Who Is Responsible for Reliability Compliance?

- **The Transmission Group** has lead responsibility for monitoring and oversight of NU's (Generation, Distribution, and Transmission) compliance with Reliability requirements.

- **Everyone** who ‘touches’ some aspect of Reliability Requirements plays a role.
  - Everyone must attain an appropriate level of understanding based on level of involvement with compliance requirements.

- **Regulations and Compliance** is responsible for:
  - Overall Reliability compliance monitoring and oversight
  - Establishing written procedures for documenting and tracking Reliability requirements
  - Enhancing the NERC Standards database
  - Developing clear Reliability compliance roles and responsibilities
  - Educating and training on the Reliability Compliance process
  - Coordinating efforts with Corporate and other TG departments as needed

- Each **Requirement “Owner”** (within or outside TG) is responsible for the implementation of the Reliability requirement, including:
  - Conducting a gap analysis and identifying risks
  - Consulting with subject matter experts
  - Educating and training on the Reliability Compliance requirements
  - Developing and executing an implementation plan
  - Reporting actions to Regulations and Compliance

- **Performance Assessment and Risk Management** is responsible for:
  - Conducting and leading team assessments
  - Identifying opportunities for improvement
  - Recommending a corrective action plan
  - Ensuring the corrective action plan is implemented
  - Reporting actions to Regulations and Compliance
Compliance Program Goals

- Develop a holistic compliance program focused on continuous performance improvement.

- Consistently meet all compliance requirements through well documented, auditable processes.

- Ensure proper maintenance of content and storage of information needed to demonstrate compliance.

- Align our organization and internal processes to foster a compliance-focused culture.
How Are We Meeting Our Compliance Goals?

- **Developing a structured Compliance Program focused on four key elements:**
  - **LEARN:** understanding compliance requirements
  - **DO:** creating a compliance-focused organization
  - **CHECK:** establishing effective internal controls
  - **SHAPE:** influencing new compliance requirements

- **Instituting procedures for becoming auditably compliant with mandatory Reliability Standards.**

- **Enhancing our Early Detection System:**
  - Transmission Regulatory Group (internal)
  - NERC Compliance Oversight Committee (internal)
  - External committee participation

- **Strengthening and formalizing our Regulatory Advocacy outreach**
  - Relationship Management
    - NERC, ISO-NE, NEPOOL, NAESB, PTO-AC, NPCC, NESCOE
  - Internal Coordination
    - Regulatory Affairs, Governmental Affairs, Utility Group, Shared services
Our Compliance Program Is Aligned with NU’s 10-Point Program
Compliance Program documentation addresses:

- Compliance Procedures
- Quality Assurance Process
- Compliance Calendar
- Performance Management System
- Training Programs
- Issue Management Plans
- Relationship Management Plans

Compliance Program Overview
- Transmission Regulatory Group
- NERC Compliance Oversight Committee
- NERC/NPCC Committee Working Group

Compliance Schedule
Compliance Procedure Requirements
New Compliance Requirements
Individual Management Plans
Gap Analysis
Reliability Database
Balloting Database
Self-Certification
Self-Reporting Investigation

Compliance Schedule Preparation
Quality Assurance-Regulatory Auditable Records
Quality Assurance-Reliability TBD
Cyber Security Compliance Program

“Steps to Success”
Steps to Success

• **Timeline**
• **Governance Model**
• **Critical Decision making**
• **Assessments**
• **Sign – Off process**
• **Brief Management Committee**
  – *Conduct one-on-one meetings with all officers*

• **Assign Program Manager**
  – *High Level of confidence from your officer team needed in this person*

• **Develop Teams**
  – *Officers must assign team members to ensure commitment*

• **Official Project Kickoff Meetings**
Steps to Success

**Steps to Success**

**Schedule**

- **Begin to identify asset definitions**
  - Completed

**January**
- Identify the Critical Asset Team
  - Completed

**February**
- Develop Critical Asset Methodology
  - Completed

**May**
- Complete NU Critical Asset Identification
  - Completed

**December**
- Appoint a Oversight Committee
  - Completed

**June**
- Complete GAP Analysis and Preliminary Plan to Close Gaps
  - Working

**March**
- Identify CIP Sponsors and CIP Owners
  - Completed

**April**
- Develop Preliminary Critical Cyber Asset List
  - Completed

**August**
- Propose 2007 Project Funding

**NERC Approves and adopts CIP Standards** - June

**Transition to future owners to execute the plan**
• **Management Buy-in & Support**
  
  – **Executive Sponsor – Compliance Officer**
  – **Executive Oversight Team – VP’s**
  – **Dedicated Corporate Program Manager for Compliance Project**
  – **Management Team members designated as owners – Managers and Directors**
  – **A strong link to Committee on Internal Controls and Internal Audit**
Steps to Success
Clear roles and responsibilities

Executive Sponsor
- Oversee NU's reliability compliance program.
- Chair a cross-functional cyber security oversight committee.
- Sign off on NU's compliance.

Oversight Committee
- Oversee the process used to ensure NU's compliance with the cyber security standards.
- Set the tone for compliance.
- Prioritize remediation efforts.
- Resolve escalated issues, such as resource needs.
- Sign off on NU's compliance.

Program Manager
- Work with CIP Sponsors and CIP Owners to prepare a detailed compliance plan.
- Ensure controls are in place to effectively manage scope, costs, schedule and resources.
- Manage risk
- Monitor and report performance against the plan to the Oversight Committee
Steps to Success
Separation of duties

Critical Infrastructure Protection (CIP) Sponsors
- Typically Directors
- Oversee the work of the CIP Owner.
- Sign off on our compliance plan with the CIP standard.

Critical Infrastructure Protection (CIP) Owners
- Assess the impact of the cyber security standard on NU.
- Identify our compliance gaps.
- Develop plans to close the gaps (e.g., training, adding hardware, software, or procedures).
- Identify testing needs, execute the tests, and document the tests and the results.
- Identify actions required to fully comply with the standard.
• **Strong controls and process needed:**
  
  – **Definition of a “critical asset” for company**
  
  – **Selection of external consultants if recommend by management**
  
  – **Selection of a methodology to be used for risk assessments process outline within the various CIPs**
  
  – **Assignment of Compliance Officer**
  
  – **Assignment of Program Manager**
  
  – **Rigorous sign-off process**
• **Vulnerability and Risk Assessments**
  
  – Conduct strong GAP analysis
  
  – Carefully select a consultant that is respected in the industry (if recommended by management)
  
  – Develop strong documentation on internal and/or external risk assessments conducted on each CIP requirement
  
  – Strive to do more than the minimum to minimize corporate risk
  
  – Don’t just see what you want to see!
The CIP-002 Team for Northeast Utilities

Objective:
- Define Identification Methodology
- Define Critical Assets
- Define Critical Cyber Assets

Time Frame:
February 2006 – June 2006

**Critical Asset Identification Team – Director of Transmission Asset Strategy**
- Review and interpret CIP-002 which requires that we identify our critical assets.
- Identify the criteria NU will use to determine which assets will be classified as critical.
- Apply the criteria to identify which NU assets are to be classified as critical.

**Critical Cyber Asset Identification Team – Manager of Transmission Asset Management**
- Review and interpret CIP-002 which requires that we identify the critical cyber security assets.
- Identify the criteria NU will use to determine which cyber security assets will be classified as critical.
- Apply the criteria to identify which NU cyber security assets are to be classified as critical.

**Critical Asset and Critical Cyber Asset Approval Team**
8 Directors from 3 Business Group
Transmission, Utility Group and Shared Services

**Critical Asset Identification Team**
6 Managers from 3 Business Group
Transmission, Utility Group and Shared Services

**Critical Cyber Asset Identification Team**
6 Managers from 3 Business Group
Transmission, Utility Group and Shared Services
After review of a number of risk assessment methodologies, the Critical Asset and Critical Cyber Asset Approval Team determined that use of the NU Enterprise Risk Management methodology was the preferred methodology.

Source: Treasury Board of Canada & CGSO & NU ERM

Baseline Methodology & Review:
Performed at the outset of a NERC CIP Compliance Effort
• Need a strong corporate commitment to a compliance program
• Must have an aggressive but achievable timeline
• Develop a strong governance model
• Institute an effective critical decision approval process
• Do multiple level detailed assessments and gap analysis
• Management Sign – off at each step is critical
• Strive to develop action plans aligned with CIP implementation dates that management will support
Summary

• Start the process early, right away
• This is a tops down initiative
• Look to see how your company approached SOX compliance – both from a project standpoint and corporate oversight
• Need cross functional buy-in – this hit many area’s in the company.
• Communications, communications, communications
• Documentation, documentation, documentation
• Prioritize and set out multi-year achievable plans to management
Questions ?