Operations & Planning Compliance Issues and Observations

November 2014
Compliance Workshop
Cambridge, MA

Ben Eng
Manager, Compliance Audits and Investigations Operations and Planning
Agenda

• Introductions –
  • Roles and Responsibilities
  • Recent/Planned Activities

• 2015 RAI Implementation
  • CMEP IP – NERC and NPCC
  • Risk Elements, IRA, ICE and Scoping
  • Auditor Tools and Processes

• General Auditor Observations and Experiences
  • Audit Documentation Submittals
  • Quality of Evidence
  • Audit Timeline

• Auditor Observations – specific standards
Auditors

• Operations and Planning (O&P)
  • Ben Eng (Audit Manager)
  • Garth Arnott (Lead Auditor)
  • Richard Burke (Lead Auditor)
  • Mike Calimano (Lead Auditor)
  • Phil Creech (Lead Auditor)
  • Anthony Giasi (Lead Auditor)
  • John Malgeri (Lead Auditor)
  • Kim Pitchell (Lead Auditor)
  • John Ravalli (Lead Auditor)
Auditors

• Roles and Responsibilities
  • Implement RAI for all Ops & Planning (a.k.a “non-CIP”) NERC Reliability standards being monitored
  • Onsite/Offsite Audits
  • Spot Checks
  • Compliance Investigations
  • Support Certification Reviews - qualifying changes to existing BA/RC/TOP
  • Support upcoming full Certifications for new TOPs
  • Support Corroborating Evidence Interpretation (CEI) with ISONE and NYISO
• **Recent Activities**

**2014**
- 34 offsite O&P, and 5 onsite O&P audits – Scheduling, Risk Assessments, Scoping, and Performance of Audit
- Support the O&P portion of 7 onsite and ~31 offsite CIP audits
- Support 2 Certification Reviews
- Spot Checks – 35 entities, 473 requirements/sub-requirements

**2015** (planned)
- 34 offsite O&P, and 4 onsite O&P audits – Scheduling, RAI, IRA, ICE (optional), Scoping, and Performance of Audit
  - Some of these for Canadian Provinces
  - NPCC is unique in auditing French speaking entities
- Support Certification of new TOPs
Audit Timing Overview and Milestones (revised for RAI)

• 2015 Audit Schedule for NPCC audits (offsite/onsite, O&P/CIP)
  o Already posted in November 2014.
  o Gives entities advance notice of 2015 scheduled audits.
  o Entities may ask for adjustments due to asset transfers, outages, peak period issues.

• (RAI) NERC and NPCC CMEP Implementation Plans posted on November 19, 2014
  • NPCC CMEP IP is Appendix A3 to the NERC CMEP IP
  • Describes Risk Elements, IRA and ICE

• NPCC Auditors perform IRA

• NPCC performs ICE if entity volunteers for it.

• Rest of Audit Timing and Milestones remain the same (provided in previous NPCC Compliance Workshop presentation)
2015 RAI Implementation

• Overview provided in Sal’s presentation
• Starts with Risk Elements feeding into IRA
• (Optional) ICE flow can reduce scope, increase intervals or indicate other means of monitoring (more about this later)
Risk Elements

• 2015 NERC Risk Elements Guide says “In 2015, the ERO Enterprise identified nine risk elements with specific areas of focus. REs will consider the nine risk elements, along with regional risk considerations, to develop their Regional Implementation Plans.”

• “Regional Entities are expected to consider local risks and specific circumstances associated with individual registered entities within their footprint when developing their compliance oversight plans.”

• NPCC Auditors reviewed and modified the Risk Elements to customize for NPCC entities

• NPCC CMEP IP lists the Regional Risks and Associated Reliability Standards Subject to Regional Monitoring
Risk Elements


- Section 3, *Regional Risks and Associated Reliability Standards*, should be a very close approximation for
  - your 2015 audit scope, or
  - what you may be asked to Self-Certify compliance with for the monitoring period 2015, or
  - one or more things your entity may be Spot Checked for during 2015

- What can change the list?
Inherent Risk Assessments (IRA)
Auditor Tools and Processes

Inherent Risk Assessment

- NPCC refined the 2014 template and has used for 2015.

<table>
<thead>
<tr>
<th>A</th>
<th>B</th>
<th>C</th>
<th>D</th>
<th>E</th>
<th>F</th>
<th>G</th>
<th>H</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>NPCC Entity Risk Assessment Template</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Purpose - To document the risk review of the entity’s scheduled for 2015 audits and determine if a recommendation should be made to expand the audit scope.</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Entity Risk Rating</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Entity Impact</td>
<td>Low</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>final determination</td>
</tr>
<tr>
<td></td>
<td>BES Impact</td>
<td>Low</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>final determination</td>
</tr>
<tr>
<td><strong>Company</strong></td>
<td>Name</td>
<td>Document</td>
<td>Document/File Location</td>
<td>Document/File Location</td>
<td>Document/File Location</td>
<td>Comments</td>
<td></td>
</tr>
<tr>
<td>11</td>
<td>NCR Number</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>12</td>
<td>Registered Functions</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>13</td>
<td>Registration date</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>14</td>
<td>Ownership change (Previous Owner/Time Period)</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>15</td>
<td>Company Profile</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Q:\Audits\2011 Company Profiles\</td>
<td></td>
</tr>
<tr>
<td>16</td>
<td>Culture of Compliance Survey</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Q:\DRA\Culture of Compl Surveys 2011\</td>
<td></td>
</tr>
<tr>
<td>17</td>
<td>One-line Diagram</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>18</td>
<td>Scheduled Audit Date</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
### Inherent Risk Assessment (cont’d)

<table>
<thead>
<tr>
<th></th>
<th>A</th>
<th>B</th>
<th>C</th>
<th>D</th>
<th>E</th>
<th>F</th>
<th>G</th>
<th>H</th>
</tr>
</thead>
<tbody>
<tr>
<td>21</td>
<td>Previous Reviews</td>
<td></td>
<td></td>
<td>Document</td>
<td>Document/File Location</td>
<td>Document/File Location</td>
<td>Document/File Location</td>
<td>Comments</td>
</tr>
<tr>
<td>22</td>
<td>Audits</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>23</td>
<td></td>
<td></td>
<td>Previous Audits</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>24</td>
<td></td>
<td></td>
<td>Possible Violations</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>25</td>
<td></td>
<td></td>
<td>Recommendations</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>26</td>
<td></td>
<td></td>
<td>Culture of Compliance</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>27</td>
<td>Spot Checks</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>28</td>
<td></td>
<td></td>
<td>Previous Spot Checks</td>
<td></td>
<td></td>
<td>Q:\CM\SpotChecks</td>
<td></td>
<td></td>
</tr>
<tr>
<td>29</td>
<td></td>
<td></td>
<td>Possible Violations</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>30</td>
<td></td>
<td></td>
<td>Recommendations</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>31</td>
<td></td>
<td></td>
<td>Culture of Compliance</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>32</td>
<td>Self Reports</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>33</td>
<td></td>
<td></td>
<td>Report details</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>34</td>
<td></td>
<td></td>
<td>Mitigation Plan</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>35</td>
<td></td>
<td></td>
<td>Mitigation Plan Status</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>36</td>
<td>Self Certifications</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>37</td>
<td></td>
<td></td>
<td>Timeliness</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>38</td>
<td>Compliance Investigations</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Q:\CM\Investigations</td>
<td></td>
<td></td>
</tr>
<tr>
<td>39</td>
<td></td>
<td></td>
<td>Report</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>40</td>
<td></td>
<td></td>
<td>Findings</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>41</td>
<td></td>
<td></td>
<td>Resolution</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
# Inherent Risk Assessment (cont’d)

<table>
<thead>
<tr>
<th></th>
<th>A</th>
<th>B</th>
<th>C</th>
<th>D</th>
<th>E</th>
<th>F</th>
<th>G</th>
<th>H</th>
</tr>
</thead>
<tbody>
<tr>
<td>46</td>
<td>Internal Controls</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>47</td>
<td></td>
<td>Report</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>48</td>
<td></td>
<td>Other</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>50</td>
<td>Mis-operations</td>
<td>Report</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>51</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Q:\Audits\PRC004_Misoperation Reports</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>52</td>
<td>EOP-004 Reports</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Q:\Audits\EOP004_Disturbance Reporting</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

## Entity Impact on the Interconnection

<table>
<thead>
<tr>
<th></th>
<th>Document/File Location</th>
<th>Document/File Location</th>
<th>Document/File Location</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>57</td>
<td>Company Profile</td>
<td>Q:\Audits\2011 Company Profiles</td>
<td>Previous report or spot check</td>
<td></td>
</tr>
<tr>
<td>58</td>
<td>Generation</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>59</td>
<td>Transmission</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>60</td>
<td>Critical Facilities</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>61</td>
<td>SPS</td>
<td>Q:\Audits\SPS List_CEII</td>
<td></td>
<td></td>
</tr>
<tr>
<td>62</td>
<td>A10 list</td>
<td>Q:\Audits\A10 List_CEII</td>
<td></td>
<td></td>
</tr>
<tr>
<td>63</td>
<td>Key Facilities list</td>
<td>Q:\Audits\KeyFacilitiesList_CEII</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
## Inherent Risk Assessment (cont’d)

<table>
<thead>
<tr>
<th></th>
<th>A</th>
<th>B</th>
<th>C</th>
<th>D</th>
<th>E</th>
<th>F</th>
<th>G</th>
<th>H</th>
</tr>
</thead>
<tbody>
<tr>
<td>58</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>59</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>60</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>61</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>62</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>63</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>64</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>65</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>66</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>67</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>68</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>69</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>70</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>71</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>72</td>
<td></td>
<td>AML Expansion</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>73</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>74</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>75</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>76</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>77</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>78</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>79</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>80</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>81</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
## Mandatory Audit Scope (items with “R” in column E)

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>FAC-008-3</td>
<td>R1</td>
<td>Each Generator Owner shall have documentation for determining the Facility Ratings of its solely and jointly owned generator Facility(ies) up to the low side terminals of the main step up transformer if the Generator Owner does not own the main step up transformer and the high side terminals of the main step up transformer if the Generator Owner owns the main step up transformer. [See standard for documentation requirements]</td>
<td>LOWER</td>
<td>R</td>
<td>A</td>
<td>GO</td>
</tr>
<tr>
<td>PRC-001-1</td>
<td>R1</td>
<td>Each Transmission Operator, Balancing Authority, and Generator Operator shall be familiar with the purpose and limitations of protection system schemes applied in its area.</td>
<td>HIGH</td>
<td>R</td>
<td>A</td>
<td>BA, GOP, TOP</td>
</tr>
<tr>
<td>PRC-005-1b</td>
<td>R2</td>
<td>Each Transmission Owner and any Distribution Provider that owns a transmission Protection System and each Generator Owner that owns a generation Protection System shall provide documentation of its Protection System maintenance and testing program and the implementation of that program to its Regional Reliability Organization on request (within 30 calendar days). The documentation of the program implementation shall include:</td>
<td>LOWER</td>
<td>R</td>
<td>A</td>
<td>DP, GO, TO</td>
</tr>
<tr>
<td>PRC-023-1</td>
<td>R1</td>
<td>Each Transmission Owner, Generator Owner, and Distribution Provider shall use any one of the following criteria (R1.1 through R1.13) for any specific circuit terminal to prevent its phase protective relay settings from limiting transmission system loadability while maintaining reliable protection of the Bulk Electric System for all fault conditions. Each Transmission Owner, Generator Owner, and Distribution Provider shall evaluate relay loadability at 0.85 per unit voltage and a power factor angle of 30 degrees. [Mitigation Time Horizon: Long Term Planning]</td>
<td>HIGH</td>
<td>R</td>
<td>A</td>
<td>TO, GO, DP</td>
</tr>
<tr>
<td>PRC-023-1</td>
<td>R1.1</td>
<td>Set transmission line relays so they do not operate at or below 150% of the highest seasonal Facility Rating of a circuit, for the available defined loading duration nearest 4 hours (expressed in amperes).</td>
<td>No Individual VRF Assigned</td>
<td>R</td>
<td>A</td>
<td>TO, GO, DP</td>
</tr>
<tr>
<td>PRC-023-1</td>
<td>R1.2</td>
<td>Set transmission line relays so they do not operate at or below 115% of the highest seasonal 15-minute Facility Rating2 of a circuit (expressed in amperes).</td>
<td>No Individual VRF Assigned</td>
<td>R</td>
<td>A</td>
<td>TO, GO, DP</td>
</tr>
</tbody>
</table>
## Expanded for Audit Scope (items with “E” in column E)

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>CIP-001-2a</td>
<td>R1.</td>
<td>Each Reliability Coordinator, Balancing Authority, Transmission Operator, Generator Operator, and Load-Serving Entity shall have procedures for the recognition of and for making their operating personnel aware of sabotage events on its facilities and multi-site sabotage affecting larger portions of the Interconnection.</td>
<td>MEDIUM</td>
<td></td>
<td></td>
<td>BA, GOP, LSE, RC, TOP</td>
<td></td>
</tr>
<tr>
<td>4</td>
<td>CIP-001-2a</td>
<td>R2.</td>
<td>Each Reliability Coordinator, Balancing Authority, Transmission Operator, Generator Operator, and Load-Serving Entity shall have procedures for the communication of information concerning sabotage events to appropriate parties in the Interconnection.</td>
<td>MEDIUM</td>
<td></td>
<td></td>
<td>BA, GOP, LSE, RC, TOP</td>
<td>Located in Zone J</td>
</tr>
<tr>
<td>5</td>
<td>CIP-001-2a</td>
<td>R3.</td>
<td>Each Reliability Coordinator, Balancing Authority, Transmission Operator, Generator Operator, and Load-Serving Entity shall provide its operating personnel with sabotage response guidelines, including personnel to contact, for reporting disturbances due to sabotage events.</td>
<td>MEDIUM</td>
<td></td>
<td></td>
<td>BA, GOP, LSE, RC, TOP</td>
<td>Located in Zone J</td>
</tr>
<tr>
<td>6</td>
<td>CIP-001-2a</td>
<td>R4.</td>
<td>Each Reliability Coordinator, Balancing Authority, Transmission Operator, Generator Operator, and Load-Serving Entity shall establish communications contacts, as applicable, with local Federal Bureau of Investigation (FBI) or Royal Canadian Mounted Police (RCMP) officials and develop reporting procedures as appropriate to their circumstances.</td>
<td>MEDIUM</td>
<td></td>
<td></td>
<td>BA, GOP, LSE, RC, TOP</td>
<td>Located in Zone J</td>
</tr>
<tr>
<td>7</td>
<td>COM-002-2</td>
<td>R1.</td>
<td>Each Transmission Operator, Balancing Authority, and Generator Operator shall have communications (voice and data links) with appropriate Reliability Coordinators, Balancing Authorities, and Transmission Operators. Such communications shall be staffed and available for addressing a real-time emergency condition.</td>
<td>HIGH</td>
<td></td>
<td></td>
<td>BA, GOP, TOP</td>
<td>Multi units staffing unknown</td>
</tr>
<tr>
<td>8</td>
<td>EOP-005-2</td>
<td>R13.</td>
<td>Each Transmission Operator and each Generator Operator with a Blackstart Resource shall have written Blackstart Resource Agreements or mutually agreed upon procedures or protocols, specifying the terms and conditions of their arrangement. Such Agreements shall include references to the Blackstart Resource testing requirements. [Violation Risk Factor = Medium] [Time Horizon = Operations Planning]</td>
<td>MEDIUM - Pending</td>
<td></td>
<td></td>
<td>GOP, TOP</td>
<td>Not in NYISO plan but part of Con Ed plan</td>
</tr>
<tr>
<td>11</td>
<td>EOP-005-2</td>
<td>R14.</td>
<td>Each Generator Operator with a Blackstart Resource shall have documented procedures for starting each Blackstart Resource and energizing a bus. [Violation Risk Factor = Medium] [Time Horizon = Operations Planning]</td>
<td>MEDIUM - Pending</td>
<td></td>
<td></td>
<td>GOP</td>
<td>Not in NYISO plan but part of Con Ed plan</td>
</tr>
</tbody>
</table>
2015 RAI Results

• Completed IRA and ICE applied to initial scope of audit to determine final scope.
• Final scope attached to Audit Notification Letter.
Other Auditor Observations and Practices
PRC-002-NPCC-01, Disturbance Monitoring Equipment

Status
Currently doing audits/spot checks for 75% Implementation. 100% implementation is on October 20, 2015

Challenges to Entity
• Discern and provide evidence that 75% criteria is being met.
• Criteria varies for each requirement
• A-10 only for Transmission (per CGS-005) and CGS-002
• Guidance is not self contained in Regional Standard - Webinars and Q&A, Requests for Interpretations and NPCC Compliance Guidance Statements
• First time audit of first Regional Reliability Standard

Challenges to Auditors
• All of the above
• Variety of approaches to processing audit information
• Learning curve for processing, efficiencies and consistency to roll into future audits.
General Auditor Experiences and Observations

- Read the Notification Letter carefully
- Do not send documents (i.e. completed pre-Audit surveys) as attachments to emails. Send to ftp site as requested by letter.
- Problems sending audit files to NPCC FTP site? Consult your IT department to ensure there are no size limitations for sending out files
General Auditor Experiences and Observations

Discovery of possible non-compliances after receipt of Audit Notification Letter

• Directions are in the Audit Notification Letter
• Contact the Lead Auditor ASAP to discuss
• Provide as much info as possible to Lead Auditor and Audit Manager so that they can determine when and what level of detail you should provide on the Non-Compliance Tracking sheet
General Auditor Experiences and Observations

Documentation

• RSAW narratives are generally good. Best ones have clear, concise statements citing relevant sections of evidence to directly demonstrate compliance.

• Read the Audit Approach sections of the RSAW to understand Auditors’ expectations for narrative and supporting documentation.

• Do an independent review. Preferably by someone who is not a Subject Matter Expert.
General Auditor Experiences and Observations

Documentation (cont’d)

• Do an overall quality check – is all the evidence there to correlate with the RSAW or Evidence Tracking Sheet data request? Right version of RSAW?

• Is all the documentation provided when responding to RSAWs or ETS questions?

• Information gaps and missing/inaccurate ratings of one or more pieces of equipment in the most limiting element series analysis, (FAC-008)

• Missing/Inaccurate equipment listings and explanations/annotations (PRC-005)
General Auditor Experiences and Observations

Suggestions:

• If unsure, obtain early clarification for what elements are material to the BES (hence within scope of the audit)
• Provide more evidence demonstrating use of procedures in lieu of long RSAW narratives.
• SMEs should be familiar with audit documentation.
• Review compliance obligations for transfer of ownership of existing assets that are material to, or affecting reliability of, the BES

QUESTIONS ?
Thank You
CIP Compliance Issues and Observations

NPCC CIP Audit Team

Fall 2014 Compliance and Standards Workshop
Classroom Session – November 20, 2014
Agenda

• Introduction of CIP Audit Team.
• CIP Transition Guidance
• CIP Version 5 Summary of Lessons Learned and FAQs.
• TFE’s In Version 5.
• Q&A
The CIP Audit Team

Staff
John Muir – jmuir@npcc.org
David Cerasoli – dcerasoli@npcc.org
Daniel Grinkevich – dgrinkevich@npcc.org
Marie Kozub – mkozub@npcc.org
Peter Scalici – pscalici@npcc.org

Contract Auditors
Val Ayers
Lee Budd
Frank Lembo
Wayne Lewis

NPCC Main Number: 212-840-1070
Compliance Timeline

Effective Date for Compliance with all non-periodic requirements are:

- April 1, 2016 for High and Medium Impact
- April 1, 2017 for Low Impact

Effective date for compliance with initial performance of periodic requirements is April 1, 2016.
CIP Transition Guidance
Critical Asset Identification

Option 1:
Continue to maintain a valid Risk-Based Assessment Methodology (RBAM) pursuant to CIP-002-3, Requirement R1.
- The RBAM must include a procedure for conducting the risk-based assessment.
- The RBAM must include appropriate and justified evaluation criteria for each type of asset being considered.
- The RBAM must be reviewed and approved annually.
- The RBAM must be applied at least annually to derive a list of Critical Assets.
Option 2:

Responsible Entities that have already adopted the CIP V4 Critical Asset Criteria (CIP-002-4, Attachment 1), may continue to use the CIP V4 Critical Asset Criteria in lieu of maintaining a RBAM.

- Adoption of the V4 Critical Asset Criteria must have occurred before August 12, 2014.
- Critical Assets identified per criterion 1.4 (Blackstart Resources) and criterion 1.5 (Cranking Paths) will not be subjected to the CIP V3 Standards, but Transmission Operator Control Centers controlling cranking path assets will continue to be treated as Critical Assets.
- Annually approve the adoption of the V4 Critical Asset Criteria.
Option 3:
Responsible Entities may adopt the CIP V5 “High” and “Medium” Impact Rating Criteria (CIP-002-5.1, Attachment 1) to identify Critical Assets in lieu of maintaining a RBAM.

- May adopt the V5 Impact Rating Criteria at any time.
- May immediately apply the V5 Impact Rating Criteria to derive a new Critical Asset list.
- May immediately remove Critical Assets and associated Critical Cyber Assets from the Critical Asset list that do not satisfy any of the V5 High or Medium Impact Rating Criteria.
- Annually approve the adoption of the V5 Impact Rating Criteria.
During the Transition Period:

On-site CIP compliance audits of Responsible Entities registered as RCs, BAs, TOPs and other Responsible Entities with Critical Cyber Assets will continue.

Off-site CIP compliance audits of Responsible Entities with no Critical Cyber Assets (other than RCs, BAs, or TOPs) are cancelled.

- Self-reports, spot checks, and self-certifications still allowed.
- Audits of “off-site entities” may resume with CIP V5.
CIP Transition Guidance
Compliance Monitoring During the Transition Period

Responsible Entities audited during the Transition Period may choose to be audited against the CIP V3 or CIP V5 Standards.

- Election made on requirement-by-requirement basis.
- Election may be made on a site-by-site basis.

Request for Information will be issued prior to issuance of the audit notification.

- Regions will issue a spreadsheet with selection options.
- Entities will have 15 days to respond.
CIP Version 5 Summary of Lessons Learned and FAQs.

Lessons Learned involve increased technical discussion and analysis. Lessons Learned and FAQs are subject to industry comment and input. Almost half of these questions relate to CIP-002-5.1 - BES Cyber System Categorization.

CIP-002-5 R1: Impact rating of generation resources (Comments by 11/14)
What options are available to categorize the impact rating of BES Cyber Assets at plants greater than 1500 MW?

CIP-002-5 R1: Relay protection in substations with different impact ratings (Comments by 11/14)
How should the impact rating of line protection relays at each end of a transmission line connecting two substations be determined?

CIP-002-5 R1: Programmable electronic devices
What are some practical examples for what is or is not a programmable electronic device?

CIP-005-5 R1: Virtual server and network environments
How can virtual environments that physically reside inside and outside an Electronic Security Perimeter be secured and considered compliant?
CIP Version 5 Summary of Lessons Learned and FAQs.

CIP-002-5 R1: BES impact of transmission scheduling systems
Should transmission scheduling systems be considered medium- or high-impact rating BES Cyber Systems?

CIP-002-5 R1: Identifying BES Cyber Systems and BES Cyber Assets
What are some practical approaches to identify BES Cyber Systems and BES Cyber Assets?

CIP-002-5 R1: Distributed BES Cyber Assets at generating plants and substations
Are instrumentation devices such as sensors, actuators, and controllers considered to be programmable electronic devices? If so, what methods would be appropriate to secure them from a compliance perspective?

CIP-002-5 R1: Grouping BES Cyber Assets
What are the advantages of grouping BES Cyber Assets into BES Cyber Systems, and how can this help demonstrate compliance?

CIP-002-5 R1: Shared equipment at a substation
What issues need to be addressed related to substations that are shared by different Entities?
CIP Version 5 Summary of Lessons Learned and FAQs.

CIP-002-5 R1: Applicability of Control Centers to Transmission Operators (TOP) and Transmission Owners (TO)
How would CIP-002-5 Attachment 1 criterion 2.12 apply to medium-impact Control Centers if the functional obligations are performed by the TO on behalf of the TOP?

CIP-002-5 R1: Generation Interconnection points
Clarify the terms “generation interconnection point,” “generation interconnection Facility,” and “collector bus” for the purposes of applying CIP-002-5 Attachment 1 impact rating criteria 2.1 and 2.2.

CIP-003-5 R2: Medium-impact rating, non-routable, no dial-up access Cyber Assets
What is the complete set of CIP Version 5 requirements that apply to BES Cyber Systems without routable or dial-up access?.

CIP-002-5 R1.2: Serial devices with External Routable Connectivity
Are serial based systems with local serial connections considered to have External Routable Connectivity if they are remotely accessible via routable protocol?
CIP Version 5 Summary of Lessons Learned and FAQs.

CIP-005-5 R1.5: Intrusion detection systems
Discuss the merits of installing intrusion detection systems outside the Electronic Security Perimeter.

CIP-005-5 R2: Interactive remote access
What needs to be considered to determine if an electronic connection is Interactive Remote Access?

CIP-005-4: Electronic Access Monitoring and Control Systems
How should mixed-trust authentication processes be managed to ensure compliance?

CIP-006-5 R1: Multiple physical access controls (FAQ)
Discuss options for using two or more physical access controls for high-impact BES Cyber System Physical Security Perimeters.

CIP-007-5 R1: Protecting physical ports (FAQ)
How can tamper tape be used to protect physical ports to comply with this requirement?
CIP Version 5 Summary of Lessons Learned and FAQs.

**CIP-007-5 R2: Identifying sources for patch management (FAQ)**
How should the appropriate sources for obtaining security patches be determined and documented?

**CIP-007-5 R3.2: Mitigate the threat of detected malicious code (FAQ)**
Clarify if entities are required to mitigate the threat of detected malicious code regardless of the methods they choose to deter, detect, or prevent malicious code.

**CIP-010-2 R1: Change management**
What are some methods to automate the change and configuration management process for substation equipment?

**CIP-010-2 R3: Vulnerability testing of Physical Access Control Systems (FAQ)**
How should active vulnerability scans be managed for Physical Access Control Systems given their sensitivity to denial of service attacks?

**CIP-010-2 R4: Protection of transient devices (FAQ)**
What are the protection requirements for transient devices used for maintenance activities?
TFE’s and Version 5

Version 5 Requirements that allow for TFE’s

Need to terminate Version 3 TFE’s
TFE’s and Version 5

Version 5 Requirements that allow for TFE’s

<table>
<thead>
<tr>
<th>V5 TFEs not associated with V3 TFEs</th>
</tr>
</thead>
<tbody>
<tr>
<td>CIP-005-5</td>
</tr>
<tr>
<td>-----------</td>
</tr>
<tr>
<td>R1.4</td>
</tr>
<tr>
<td>R2.1</td>
</tr>
<tr>
<td>R2.2</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>V5 TFEs pertinent to V3 TFEs</th>
</tr>
</thead>
<tbody>
<tr>
<td>V5</td>
</tr>
<tr>
<td>-----------------------------</td>
</tr>
<tr>
<td>CIP-005-5 R2.3</td>
</tr>
<tr>
<td>CIP-007-5 R1.1</td>
</tr>
<tr>
<td>CIP-007-5 R4.3</td>
</tr>
<tr>
<td>CIP-007-5 R5.6</td>
</tr>
</tbody>
</table>
TFE’s and Version 5

- Need to terminate Version 3 TFE’s

<table>
<thead>
<tr>
<th>V3 TFEs superseded when V5 is Implemented</th>
<th>CIP-005-3</th>
<th>CIP-006-3</th>
<th>CIP-007-3</th>
</tr>
</thead>
<tbody>
<tr>
<td>R3.1</td>
<td>R1.1</td>
<td>R3.2</td>
<td></td>
</tr>
<tr>
<td></td>
<td>R4</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>R5.3</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>R 5.3.1</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>R 5.3.2</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>R6</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Questions?
Con Edison of New York Internal Controls for NERC Compliance

Peter Yost
Manager, Standards and Compliance
Con Edison Company of New York, Inc.
Corporate Organization

Con Edison, Inc. (CEI)

Regulated Utilities

Con Edison of New York (Con Edison)

Orange and Rockland

Competitive Energy Businesses

Con Edison Solutions
Con Edison Energy
Con Edison Development

Retail
Wholesale
Asset Ownership and Operator
Con Edison Delivers Energy To New York City And Westchester County

- 3.3 million electric customers
- 1.1 million gas customers
- 1,700 steam customers
- Peak 13,322 MW
- 700 MW of generation
- 37,000 miles of overhead transmission and distribution lines
- 97,000 miles of underground transmission and distribution lines
- 4,000 miles of gas mains
- 100 miles of steam mains and lines
Con Edison NERC Registration

• Con Edison is registered with NERC under the following entity types:
  – Transmission Owner
  – Load Serving Entity
  – Distribution Provider
  – Generation Owner
  – Generation Operator
  – Purchasing Selling Entity
• Future (July 2016) registration will include:
  – Transmission Operator
  – Transmission Planner
• Con Edison has requested certification as TOP
Agenda

• Compliance Organization
• Internal Compliance Program (ICP)
• Assignment of Standards to Officers
• Internal Compliance Assessments
• Managing Allegations of Non-Compliance
• Key Performance Indicators
• Compliance Tools
• COM-002
• Compliance Control Procedures
• Compliance Coordination
• Standards Development Process
• NERC Event Analysis Process
Compliance Management

- Centralized Standards and Compliance Section
  - Within System & Transmission Operations Department
  - Manager and 5 FTEs
  - Staffed by degreed engineers
- Department-based Compliance Management
  - System Operation
  - Substation Operations
  - Steam Operations
  - Central Engineering

[Diagram showing organizational structure with roles: Manager, Sr. Engineer, Engineer, Associate Engineer]
NERC and FERC have identified ICPs as critical to ensuring an entity’s reliability compliance.


EP-7560-7:
- Identifies compliance processes, practices and responsibilities
- Approved by Vice President of System and Transmission Operations
- Updated annually
- Provided to officers, SMEs, legal staff
- Posted to shared folder
Internal Compliance Program

• The ICP is posted to a shared folder along with a list of responsible Vice-Presidents and SMEs to ensure high visibility of the program
  – The list of VPs and SMEs includes all individuals with compliance responsibility for NERC Reliability Standards
• Shared folder expires every 3 months
• Folder is renewed and announcement email distributed
Below is a link to Con Edison’s Internal Compliance Program for NERC Reliability Standards, EP-7560-7 (Management of the Compliance Process for NERC and NPCC Reliability Standards). Also provided at the link is a list of Con Edison personnel who are responsible for maintaining compliance with NERC Reliability Standards or who are Subject Matter Experts and compliance evidence providers (SMEs). These documents are provided for your information. Please note that EP-7560 is confidential and should not be distributed outside of Con Edison.

These documents are being provided to you to increase the visibility of the Company’s NERC Compliance program and to share with you the program established for management of the NERC compliance process. You are receiving this as you either certify compliance with NERC Standards or serve as an SME for one or more NERC Standards.

Thank you.

David Balban  
*Engineer, Standards & Compliance*  
Transmission Planning  
Consolidated Edison Company of NY, Inc.  
4 Irving Place, Room 1300 NW  
New York, NY 10003  
212-460-1078  

\coned\corp\public\B\S-1-5-21-39997874-457639419-701057205-180124\EP-7560 Management of Compliance with NERC Reliability Standards
Major Elements of ICP

- Assignment of Standards and Requirements to Officers
- Self Certification Process
- NPCC On Site, Off Site, and Spot Check Audits
- Managing Non-Compliance Allegations
- Development of Mitigation Plans
- Managing NERC Alerts
- Standards development program
- Event reporting and analysis
Assignment of Standards to Officers

• Standards and Compliance (S&C) Section assigns an officer with compliance responsibility for each Requirement of each Standard
• One officer assigned compliance responsibility for each entity type applicable to Con Edison
  – Some Requirements have multiple officers
• Assignment to officers typically made before the Standard goes to NERC Board for approval
• S&C team seeks to identify most appropriate assignment based on functional responsibilities
### Assignment of Compliance Responsibilities to Officers

<table>
<thead>
<tr>
<th>#</th>
<th>ID</th>
<th>Standard</th>
<th>Responsible Officer: by Entity Type</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td>TO</td>
</tr>
<tr>
<td>----</td>
<td>--------</td>
<td>-----------------------------------------------</td>
<td>---------</td>
</tr>
<tr>
<td>1</td>
<td>BAL-005-0.2b</td>
<td>Automatic Generation Control</td>
<td>VP Energy Management</td>
</tr>
<tr>
<td>2</td>
<td>COM-002-2</td>
<td>Communications and Coordination</td>
<td>VP System &amp; Transmission Operations</td>
</tr>
</tbody>
</table>
NERC Standards by Organization

Chairman of the Board and Chief Executive Officer

Vice President and General Auditor

President

President Shared Services

Senior Vice President of Electric Operations

Senior Vice President of Central Operations

Vice President of Engineering and Planning

Vice President of Central Engineering

Vice President of Steam Operations

Vice President of Substation Operations

Vice President of System and Transmission Operations

Vice President of Energy Management

MOD-019
MOD-020

FAC-008
PRC-002-NPCC
PRC-004
PRC-016
PRC-018
PRC-023

CIP-002/009
BAL-005
EOP-005
FAC-003
IRO-001
IRO-010
MOD-025
PRC-001
PRC-005
PRC-015
PRC-016
PRC-017
TOP-002
VAR-002

CIP-002/009
EOP-005
PRC-005
PRC-008
PRC-011
PRC-017

COM-002
PRC-006
CIP-002/009
PRC-010
EOP-004
PRC-015
FAC-001
PRC-021
FAC-002
PRC-022
FAC-003
TOP-001
IRO-001
TOP-002
IRO-005
TOP-003
IRO-010
MOD-010
MOD-012
NUC-001

BAL-005
MOD-017
EOP-002
MOD-018
INT-004
MOD-021
IRO-001
TOP-005
IRO-005
TOP-006
MOD-004
VAR-001
Internal Compliance Assessments

- Internal Auditing Department periodically conducts audits of compliance with NERC Reliability Standards
  - Standards to be audited are based on annual audit plan
  - Consider risks identified corporately and by departments
  - Conducted like an NPCC audit: RSAWs completed and evidence prepared
  - Performed on and off site
  - Typically provide SMEs with less preparation time than a Spot Check
- Periodic NYS Department of Public Service (DPS) audits on CIP Standards
- Other:
  - S&C Section has conducted compliance assessments following system events
  - Some departments with compliance responsibility for NERC Standards conduct self-audits
Auditing NERC Standards: Priority List

From: [Redacted]  
To: [Redacted]  
Sent: Fri 4/10/2013 11:58 AM  
Subject: RE: Updated Priority List of NERC Standards

<table>
<thead>
<tr>
<th>Rank</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>C</td>
<td>Cyber security (CIP) Standards (priority ranking among the CIP standards to be determined by Auditing)</td>
</tr>
<tr>
<td>1</td>
<td>Highest priority, Standards that are frequently the focus of FERC and NERC attention, Vegetation Management, Protection System misoperations, Protection System maintenance and testing or nuclear generation.</td>
</tr>
<tr>
<td>2</td>
<td>Standards that are on NERC’s Actively Monitored List (AML) for 2014. The AML Standards are subject to self certification and audit in 2014.</td>
</tr>
<tr>
<td>3</td>
<td>Standards that are not AML but are not priority 4.</td>
</tr>
<tr>
<td>4</td>
<td>Lowest priority, Standards that are not applicable to the Company or where we have a corroborating evidence statement from the NYISO.</td>
</tr>
</tbody>
</table>

Note that regardless of the priority ranking, Con Edison must be in compliance with all NERC Standards at all times. We are subject to NPCC audit on any Standard at any time.

If you have any questions on the priority ranking or the list of Standards, please give me or David Balban a call.

NERC Standards  
Priority List 9...

Peter Yost  
Manager, Standards and Compliance
## Internal Compliance Assessments

<table>
<thead>
<tr>
<th>Year</th>
<th>Auditing Department Audits of Compliance with NERC Standards</th>
<th>Non-Cyber Standards Audited</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Cyber Standards Audited</td>
<td>Non-Cyber Standards Audited</td>
</tr>
<tr>
<td>2009</td>
<td>8</td>
<td>15</td>
</tr>
<tr>
<td>2011</td>
<td>-</td>
<td>16</td>
</tr>
<tr>
<td>2012</td>
<td>2</td>
<td>3</td>
</tr>
<tr>
<td>2013</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>2014</td>
<td>1</td>
<td>8</td>
</tr>
<tr>
<td></td>
<td>Standard</td>
<td>Title</td>
</tr>
<tr>
<td>----------------</td>
<td>----------</td>
<td>----------------------------------------------------------------------</td>
</tr>
<tr>
<td>IT Audit 14-09</td>
<td>CIP-005-3</td>
<td>Cyber Security – Electronic Security Perimeter(s)</td>
</tr>
<tr>
<td>Operational Audit 14-15</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Standard</td>
<td>Title</td>
<td></td>
</tr>
<tr>
<td>----------</td>
<td>--------</td>
<td></td>
</tr>
<tr>
<td>EOP-004-2</td>
<td>Event Reporting</td>
<td></td>
</tr>
<tr>
<td>FAC-003-1</td>
<td>Transmission Vegetation Management Program</td>
<td></td>
</tr>
<tr>
<td>FAC-008-3</td>
<td>Facility Ratings</td>
<td></td>
</tr>
<tr>
<td>IRO-001-1.1</td>
<td>Reliability Coordination – Responsibilities and Authorities</td>
<td></td>
</tr>
<tr>
<td>PRC-004-2.1a</td>
<td>Analysis and Mitigation of Transmission and Generation Protection System Misoperations</td>
<td></td>
</tr>
<tr>
<td>PRC-005-1.1b</td>
<td>Transmission and Generation Protection System Maintenance and Testing</td>
<td></td>
</tr>
<tr>
<td>PRC-008-0</td>
<td>Underfrequency Load Shedding Equipment Maintenance Programs</td>
<td></td>
</tr>
<tr>
<td>TOP-001-1a</td>
<td>Reliability Responsibilities and Authorities</td>
<td></td>
</tr>
<tr>
<td>IT Audit 13-07</td>
<td>CIP-002-3</td>
<td>Cyber Security - Critical Cyber Asset Identification</td>
</tr>
<tr>
<td>Operational Audit 12-05</td>
<td>PRC-017-0</td>
<td>Special Protection System Maintenance and Testing</td>
</tr>
<tr>
<td>IT Audit 12-07</td>
<td>CIP-007-3</td>
<td>Cyber Security - Systems Security Management</td>
</tr>
</tbody>
</table>
# Internal Compliance Assessments

<table>
<thead>
<tr>
<th>IT Audit 11-08</th>
<th>5/16/2012</th>
<th>Standard</th>
<th>Title</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>CIP-006</td>
<td>Cyber Security - Physical Security of Critical Cyber Assets</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Operational Audit 11-01</th>
<th>2/24/2012</th>
<th>Standard</th>
<th>Title</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>FAC-003-1</td>
<td>Transmission Vegetation Management Program</td>
</tr>
<tr>
<td></td>
<td></td>
<td>PRC-005-1</td>
<td>Transmission and Generation Protection System Maintenance and Testing</td>
</tr>
<tr>
<td></td>
<td></td>
<td>PRC-002-NPCC-1</td>
<td>Disturbance Monitoring</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Operational Audit 10-10</th>
<th>1/10/2011</th>
<th>Standard</th>
<th>Title</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>CIP-001-1</td>
<td>Sabotage Reporting</td>
</tr>
<tr>
<td></td>
<td></td>
<td>COM-001-1.1</td>
<td>Telecommunications</td>
</tr>
<tr>
<td></td>
<td></td>
<td>COM-002-2</td>
<td>Communications and Coordination</td>
</tr>
<tr>
<td></td>
<td></td>
<td>FAC-008-1</td>
<td>Facility Ratings Methodology</td>
</tr>
<tr>
<td></td>
<td></td>
<td>FAC-009-1</td>
<td>Establish and Communicate Facility Ratings</td>
</tr>
<tr>
<td></td>
<td></td>
<td>IRO-004-1</td>
<td>Reliability Coordination — Operations Planning</td>
</tr>
<tr>
<td></td>
<td></td>
<td>IRO-005-2</td>
<td>Reliability Coordination — Current Day Operations</td>
</tr>
<tr>
<td></td>
<td></td>
<td>PRC-001-1</td>
<td>System Protection Coordination</td>
</tr>
<tr>
<td></td>
<td></td>
<td>PRC-004-1</td>
<td>Analysis and Mitigation of Transmission and Generation Protection System Misoperations</td>
</tr>
<tr>
<td></td>
<td></td>
<td>PRC-005-1</td>
<td>Transmission and Generation Protection System Maintenance and Testing</td>
</tr>
<tr>
<td></td>
<td></td>
<td>PRC-008-0</td>
<td>Implementation and Documentation of Underfrequency Load Shedding Equipment Maintenance Program</td>
</tr>
<tr>
<td></td>
<td></td>
<td>PRC-011-0</td>
<td>Undervoltage Load Shedding System Maintenance and Testing</td>
</tr>
<tr>
<td></td>
<td></td>
<td>PRC-017-0</td>
<td>Special Protection System Maintenance and Testing</td>
</tr>
<tr>
<td></td>
<td></td>
<td>PRC-023-1</td>
<td>Transmission Relay Loadability</td>
</tr>
<tr>
<td></td>
<td></td>
<td>TOP-002-2a</td>
<td>Normal Operations Planning</td>
</tr>
<tr>
<td></td>
<td></td>
<td>VAR-002-1.1b</td>
<td>Generator Operation for Maintaining Network Voltage Schedules</td>
</tr>
</tbody>
</table>
# Internal Compliance Assessments

<table>
<thead>
<tr>
<th>Standard</th>
<th>Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>CIP-002</td>
<td>Cyber Security - Critical Cyber Asset Identification</td>
</tr>
<tr>
<td>CIP-003</td>
<td>Cyber Security - Security Management Controls</td>
</tr>
<tr>
<td>CIP-004</td>
<td>Cyber Security - Personnel &amp; Training</td>
</tr>
<tr>
<td>CIP-005</td>
<td>Cyber Security - Electronic Security Perimeter(s)</td>
</tr>
<tr>
<td>CIP-006</td>
<td>Cyber Security - Physical Security of Critical Cyber Assets</td>
</tr>
<tr>
<td>CIP-007</td>
<td>Cyber Security - System Security Management</td>
</tr>
<tr>
<td>CIP-008</td>
<td>Cyber Security - Incident Reporting and Response Planning</td>
</tr>
<tr>
<td>CIP-009</td>
<td>Cyber Security - Recovery Plans for Critical Cyber Assets</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Standard</th>
<th>Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>CIP-001-1</td>
<td>Sabotage Reporting</td>
</tr>
<tr>
<td>EOP-002-2</td>
<td>Capacity and Energy Emergencies</td>
</tr>
<tr>
<td>FAC-001-0</td>
<td>Capacity and Energy Emergencies</td>
</tr>
<tr>
<td>FAC-003-1</td>
<td>Transmission Vegetation Management Program</td>
</tr>
<tr>
<td>FAC-008-1</td>
<td>Facility Ratings Methodology</td>
</tr>
<tr>
<td>FAC-009-1</td>
<td>Establish and Communicate Facility Ratings</td>
</tr>
<tr>
<td>IRO-001-1</td>
<td>Reliability Coordination — Responsibilities and Authorities</td>
</tr>
<tr>
<td>IRO-004-1</td>
<td>Reliability Coordination — Operations Planning</td>
</tr>
<tr>
<td>IRO-005-2</td>
<td>Reliability Coordination — Current Day Operations</td>
</tr>
<tr>
<td>PRC-004-1</td>
<td>Analysis and Mitigation of Transmission and Generation Protection System Misoperations</td>
</tr>
<tr>
<td>PRC-005-1</td>
<td>Transmission and Generation Protection System Maintenance and Testing</td>
</tr>
<tr>
<td>PRC-008-0</td>
<td>Implementation and Documentation of Underfrequency Load Shedding Equipment Maintenance Program</td>
</tr>
<tr>
<td>PRC-017-0</td>
<td>Special Protection System Maintenance and Testing</td>
</tr>
<tr>
<td>TOP-001-1</td>
<td>Reliability Responsibilities and Authorities</td>
</tr>
<tr>
<td>TOP-002-2</td>
<td>Normal Operations Planning</td>
</tr>
</tbody>
</table>
NYS DPS Audits

• Staff of the New York State DPS periodically audit Con Edison on CIP Standards:

  CIP-002   October 2010
  CIP-003   October 2010
  CIP-007   October 2012
  CIP-007   July 2014
  CIP-008   March 2011
  CIP-009   July 2011
Managing Non-Compliance Allegations

• Any allegation of non-compliance should be brought to the attention of the Manager of S&C
  – Our Business Ethics and Compliance Department has program for anonymous reporting
• Manager establishes an Evaluation team including
  – Certifying officer
  – Law Department
  – Auditing Department
  – Manager of S&C
• Evaluation team reviews allegation and determines if it is credible
• Evaluation team provides assessment and recommendation to the Executive Team
Managing Non-Compliance Allegations

• Executive Team
  – President
  – Senior Vice President of Central Operations
  – Vice President of Ethics and Compliance
  – Vice President of Regulatory Services
• Executive team shall review the recommendation of the Evaluation team
• Executive Team provides guidance to Manager of S&C as appropriate
• Possible next steps if there is a determination of a violation:
  – Develop mitigation plan
  – Self-report to NPCC
  – Initiate settlement negotiations with NPCC
Managing Non-Compliance Allegations

- Notice of Alleged Violation
- Compliance Violation Investigation
- Remedial Action Directive

Audit, Complaint, or In-House Review

S&C Mgr establishes Evaluation Team

NPCC, NERC, or FERC

Executive Team
- President
- Sr. VP, Central Ops
- VP, Regulatory Svcs
- VP, Business Ethics & Compliance

NPCC

S&C Mgr, Certifying Officer, Law & Auditing
Gathers, reviews & evaluates relevant information
Managing Non-Compliance Allegations

• Implemented process on several occasions
• Evaluated possible violations of NERC Standards including:
  – CIP-004 - PRC-015
  – CIP-006 - PRC-016
  – NUC-001 - PRC-018
  – PRC-005 - FAC-008
• Self reported two violations as a result
NERC Compliance Key Performance Indicators (KPI)

• Five organizations with compliance responsibility have NERC compliance KPI
  – Central Engineering
  – Substation Operations
  – Steam Operations
  – Energy Management
  – System & Transmission Operations

• Many departments also have compliance KPIs

• KPIs typically require zero violations of NERC Standards, with certain stipulations:
  – To support a culture of compliance, KPIs do not penalize for self-reported violations

• Incorporation of NERC Compliance into KPIs is indicative of a “tone-from-the-top” internal control
Bulk Electric System (BES) Elements

• Met with NPCC to clarify list of BES transmission Elements
  – Transmission Lines
  – Transformers
  – Capacitors
  – Reactors
  – Phase Angle Regulators
• Clarified to ensure accurate BESnet data entry
System Operation Department

COM-002: Verification of Communication Protocols

• System Operation Department procedure (AD05-01-11) for verifying appropriate use of three-point or repeat-back communication for operating orders
  – Issuer delivers instruction
  – Receiver repeats back instruction
  – Issuer confirms

• All operators are reviewed twice per year to verify appropriate protocol is being followed
  – Two audio records are randomly selected for each operator
  – Use of appropriate protocol verified
  – Supplemental training is required if protocol not being followed
  – Audit form completed for all verifications
  – Operator performance scored (1 - 5 scale)
System Operation Department
Compliance Control Procedures

CIP-004
• Cyber-mandated training is managed through the Con Edison “eLearning” system
• Mandatory training reminders are sent via email, starting months in advance of due date
• Access to Critical Cyber Assets is immediately revoked if training is not completed on time

CIP-002/009
• Procedure stipulates requirements for all annual reviews
  – Critical Cyber Asset List
  – Information Protection
  – Physical security plan
  – Incident response plan
  – Vulnerability assessment
  – Back up media test
Central Engineering Department
Compliance Control Procedures

PRC-004
- Procedure CSE-01: Investigation of Automatic Power System Operations
- Requires immediate investigation of each automatic operation of protective relays
- Applied to all transmission 69 kV and above

PRC-023
- Procedure CSE-02: Relay Loadability
- Requires relay setting changes be made in accordance with PRC-023

NUC-001
- Procedure CE-0112: Indian Point Interface
- Defines responsibilities associated with NUC-001
Steam Operations Department

Compliance Control Procedures

PRC-001: Protection System Coordination
- COP 5-0-9: Managing Safety Devices on Generation Station Equipment
- CE-0110: Coordination of East River Relay Protection with NYISO
- ER-OJT-221: Familiarity with Protection Systems
- ER-OAD-005: Communication with System Operation

VAR-002: Voltage Control
- AVR status is remotely monitored at energy control center
  - AVR on/off status
  - AVR manual/auto status
- This control measure was identified in NERC ICE Guide as a corrective internal control
Compliance Tools

SharePoint
• Repository for compliance data and documentation
  – CMEP related documents
  – Audit records
  – Self certifications
  – System Events
  – BES Element lists

Action Tracking System (ATS)
• Identify and track milestones, email reminders to SMEs and compliance staff for upcoming deliverables
• Used to support compliance with the following Standards:
  – PRC-006 (UFLS)
  – PRC-006-NPCC-1 (UFLS)
  – PRC-002-NPCC-1 (DME)
  – NUC-001 (Nuclear)
  – IRO-010 (Data Coordination)
  – CIP-002 (Cyber Security)
  – CIP-003 (Cyber Security)
  – Directory 8 (Restoration)
Compliance Tools

MAXIMO

• Work management system developed by IBM
• Used to manage work planning and compliance:
  – Transmission Protection Systems
  – UFLS equipment
  – Disturbance Monitoring Equipment
• Tracks preventative and corrective maintenance on assets
• Tracks due dates for relay calibrations, trip checks, etc.
• Generates Work Orders
• Repository for all maintenance and testing records
• Generates Daily Report via email with due dates for BES and non-BES tasks
• Daily Reports distributed to responsible managers
• Department has KPI: 100% on-schedule for BES tasks
Compliance Tools

Compliance Management System (CMS)

- Application developed by System Operation SMEs
- Purpose of CMS is to support NERC compliance for the SO department
- Maintains evidence library for all standards / requirements relevant to SO
- Identifies evidence owners and prompts for updates
- CMS can use email prompts with escalation as needed
- Extensive reporting capability
- Important internal control for future TOP compliance
Compliance Coordination

- Some NERC Standards have Requirements with compliance managed by multiple Con Edison departments:
  - NUC-001
  - PRC-006
  - CIP-003
  - IRO-010
  - MOD-026/027

- Use ATS and Central Operations Procedures (COP) to manage compliance
  - Identify responsible personnel
  - Identify milestones/activities
  - Generate reminder emails
  - Follow up
Compliance Coordination

NUC-001: Nuclear
• Annual planning reviews

PRC-006: UFLS
• Coordination with NYISO

IRO-010: Data Coordination
• Timely provision of information

CIP-003: Cyber Information Protection
• Annual reviews required

MOD-026/027: Generator and Turbine Control Systems
• Requires updates to generator exciter and turbine control models
Standards Development Process

• Con Edison is an active participant in the NERC registered ballot body for the Reliability Standards

• Four members of the S&C section are segment/sector representatives in the ballot pools (TO, GO/GOP, LSE, PSE)

• One member of the S&C section actively monitors the Standards under development and coordinates with internal SMEs for voting guidance on the various projects

• S&C provides important “screening” role for Con Edison
  – Ensures SMEs are aware of Standards under development
  – Ensure Con Edison comments are shared with SDT
  – Ensures ballot body members vote and comment consistently
Standards Development Process

• Con Edison SMEs have been on various NERC Standards Drafting Teams
  – FAC five year review team (Chair)
  – IRO five year review team
  – NUC five year review team
  – Vegetation Management
  – Voltage and Reactive
  – BES Definition
  – BES Exception Process
• Con Edison also participates in NPCC Member voting
• Participate in both NPCC Regional Standards Committee and Compliance Committee
Standards Development Process

Typical Weekly Distribution

<table>
<thead>
<tr>
<th>Project #</th>
<th>Title</th>
<th>Standards</th>
<th>Action</th>
<th>Start Date</th>
<th>End Date</th>
<th>Joined Pool?</th>
<th>Ballot Recommendations</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>2010-02</td>
<td>Special Protection Systems (Phase 2 of Protection Systems)</td>
<td>Various</td>
<td>Additional Ballot and Non-Binding Pool</td>
<td>10/25/2014</td>
<td>10/29/2014</td>
<td>Yes</td>
<td>Voted “NEGATIVE” due to Implementation Plan deletion. SMEs: D. Taft, I. Vasco, A. Cardoza, M. Pacek</td>
<td>Our concern about Implementation Plans for PRC-024 and PRC-025 was included in NPCC comments. We voted &quot;NEGATIVE&quot; in the ballot.</td>
</tr>
<tr>
<td>2014-02</td>
<td>Critical Infrastructure Protection Standards Version 5 Revisions</td>
<td>Various</td>
<td>Additional Ballot and Non-Binding Pool</td>
<td>10/25/2014</td>
<td>10/29/2014</td>
<td>Yes</td>
<td>Maintaining our &quot;AFFIRMATIVE&quot; vote.</td>
<td>For comment form, L. Bukhman recommends: (1) Yes (2) N/A (3) Yes (4) N/A.</td>
</tr>
<tr>
<td>2007-06</td>
<td>System Protection Coordination</td>
<td>PRC-077</td>
<td>Informal Comment Period</td>
<td>10/1/2014</td>
<td>10/23/2014</td>
<td>N/A</td>
<td>Informal Comment period.</td>
<td>SME comments provided to NPCC on 10/16/14.</td>
</tr>
</tbody>
</table>
Event Analysis Process (EAP)

Con Edison follows the NERC EAP

- Central Operations Procedure (COP 5-0-22) to manage the EAP
- COP identified roles and responsibilities
- Coordinate activities between compliance, engineering and operations personnel
  - Identify reportable events
  - Develop event reports
  - Lessons learned
- Coordinate with external parties (NYISO, NYPA, PSE&G, etc.) to develop event reports
Notice of Penalty (NOP)
Lessons Learned Distribution

- Approximately every month NERC posts NOP, SNOP and FFT issues levied against entities
- The penalties are reviewed, summarized and lessons learned are identified
- The summaries and lessons learned are emailed to the officers and SMEs with compliance responsibility for Standards violated
- This monthly distribution maintains compliance awareness among officers and SMEs and provides an opportunity to learn from others
Website Monitoring

Daily Review for Updated Postings

- NERC.com
  - Filings
  - Lessons Learned
  - NERC Alerts
  - Compliance Process Bulletins
  - Compliance Violation Statistics
  - Enforcement and Mitigation
  - Vegetation Management Reports
  - RSAWs
  - Standards Subject to Future Enforcement

- NPCC.org
  - Compliance
  - Audit / Spot Check
  - CMEP Data Administration Application (CDAA)

- EEI Reliability postings
SUBSTATION OPERATIONS
PROCEDURE

SUBJECT: MAINTENANCE AND TESTING FOR SYSTEM RESTORATION
CRITICAL COMPONENTS

PROCEDURE NO. 0100-0047/00                  DATE ISSUED: 03/11
REVISED BY:                                PAGES: 1 of 3
                                          APPROVED BY:

1.0 PURPOSE

1.1 To maintain compliance with Northeast Power Coordinating Council (NPCC) Regional Reference Directory #8 System Restoration. The Directory requires that New York Independent System Operator (NYISO) identify Key Facilities required for restoration of the NYISO control area. The owners of Key Facilities are required to identify equipment (Critical Components) required for continued operation of the Key Facility in the event of a total loss of grid supply and shall have a maintenance and testing program for the associated equipment.

1.2 Con Edison is a member of NPCC Inc. As a member, we have the responsibility to operate the Bulk Power System in compliance with North American Electric Reliability Corporation (NERC) Reliability Standards, NPCC Regional Reliability Standards, and NPCC Criteria and Directories.

2.0 APPLICATION

2.1 This procedure is applicable to all Substation Operations personnel.

3.0 DEFINITION

3.1 Key Facilities: Facilities required to establish a basic minimum power system following a system blackout. These facilities are essential to the restoration plan of the Control Area and include generating stations, transmission elements which are part of the basic minimum power system, control centers, telecommunication centers and telecommunication facilities which are necessary to support protection and control facilities, and voice and data between the control centers and the key generating/transmission stations.

3.2 Critical Components: Equipment required for continued and proper operation of a Key Facility in the event of a total loss of AC supply. Critical components include but are not limited to blackstart generating units, substation back-up power supplies, control center and telecommunication center computer room air conditioning and telecommunication facilities back-up power supplies.
Con Edison of New York
Internal Controls
for NERC Compliance