Welcome to the Spring Workshop!

Questions or Comments?

- Email reworkshop@spp.org
- Please wait for a microphone
- Submit via online form on workshop web page (will generate email to staff from anonymous@REWWorkshop.spp.org)

Facility Information (see map on next page)

Restrooms: From the auditorium, go left out the door, then left again at the next hallway. More restrooms are located behind the stairway in the main foyer.

Vending machines: Continue past the restrooms and turn right

Business Center: Behind the reception desk. A PC and printer is available.

SPP Cafe with tables: Other side of the vending machine wall

Smoking area: Outside the SPP Cafe

Download Materials @ SPP.org ->Regional Entity ->2015 Spring Workshop:
March 10

7:30-8:00  Registration and light breakfast
8:00-8:15  Welcome  
           Gerry Burrows, SPP RE Trustee
8:15-8:55  1 - CIP Update  
           Kevin Perry, SPP RE
8:55-9:05  Break
9:05-10:25 2 - Risk-Based Compliance Monitoring Update  
           Adina Mineo, NERC
10:25-10:35 Break
10:35-11:20 3 - PRC-005-2 Effective 4/1/15  
           Louis Guidry, Cleco
11:20-11:30 Break
11:30-12:00 4 - General Manager’s Update  
           Ron Ciesiel, SPP RE
12:00-1:00 Lunch
1:00-4:40  Break-Out Sessions (see next page)
4:50-5:00  Short Q&A / Closing

March 11

7:30-8:00  Light breakfast
8:05-9:00  5 - Developments Impacting GOs/GOPs & NAGF  
           Mike Gabriel, NAGF
9:00-9:10 Break
9:10-10:10 6 - EMS-Related Lessons Learned  
           Sam Chanoski, NERC
10:10-10:20 Break
10:20-11:30 7 - Registered Entity Activities Under Risk-Based Compliance Monitoring  
           Chip Koloini, Golden Spread
           John Allen, CUS
           Bo Jones, Westar
11:45-12:00 Closing
12:00 Lunch

The RTO Forum for Members/Registered Entities begins at 1:00. Separate registration is required.
March 10 Break-Out Sessions

Seating is “first come, first serve”. Bring your questions and discussion points! We will leave the phones on in the auditorium for the CIP break-out sessions, but the other sessions will not be available via phone or webex.

1:00-2:00

| Auditorium (no limit) | Change Control and Configuration Management  
Facilitated by Steven Keller |
|-----------------------|-------------------------------------------------------------------------------------------------|
| Conf. B (limit 54)    | Inherent Risk Assessment/Internal Controls Evaluation  
Facilitated by Shon Austin, Adina Mineo, and Jim Williams |
| Conf. C (limit 45)    | PRC-023-3, PRC-004-2.1a, and PRC-025-1  
Facilitated by Mike Hughes and Greg Sorenson |

2:10-3:10

| Auditorium (no limit) | CIP Version 5 Lessons Learned and FAQ Documents  
Facilitated by Kevin Perry |
|-----------------------|-------------------------------------------------------------------------------------------------|
| Conf. B (limit 54)    | PRC-005-2  
Facilitated by Louis Guidry, Jeff Rooker, and Greg Sorenson |
| Conf. C (limit 45)    | Enforcement/Mitigation Practices and Common Issues  
Facilitated by Jenny Anderson, Joe Gertsch, and Tasha Ward |

3:10-3:40

| Snack Break and Meet & Greet with SPP staff |

3:40-4:40

| Auditorium (no limit) | CIP Open Q&A  
Facilitated by CIP Team |
|-----------------------|-------------------------------------------------------------------------------------------------|
| Conf. B (limit 54)    | Inherent Risk Assessment/Internal Controls Evaluation - Repeat  
Facilitated by Shon Austin, Adina Mineo, and Jim Williams |
| Conf. C (limit 45)    | Quarterly System Events/Event Analysis Update  
Facilitated by Alan Wahlstrom |

4:50

Return to auditorium for short closing
CIP Update

March 10, 2015

Kevin B. Perry
Director, Critical Infrastructure Protection
kperry.re@spp.org
501.614.3251
Agenda

• CIP Version 5 Transition Update
• Training and Outreach
• CIP Version 5 Revisions
• CIP-014 (Physical Protection)
• CIP Breakout Sessions
• Q&A
CIP Version 5 Transition Update

• 2015 audits
  – Entity choice: audit against V3 or V5 language
  – V5 compliance is deemed to be V3 compliance
  – Will advise entity, possibly via Area of Concern, if audited process will not be V5 compliant
  – Auditor discretion to not find V3 violation if no equivalent V5 requirement
  – Open Enforcement Actions should be mitigated to V5 requirement
  – Setting aside time for V5 outreach
CIP Version 5 Transition Update

• Two Lessons Learned approved by Standards Committee February 18, 2015, after industry comment:
  – Generation Segmentation
  – Far-End Relay

• Posted to the [NERC CIP V5 Transition web site](https://www.nerc.com) as Final Lessons Learned
CIP Version 5 Transition Update

• Three Lessons Learned recently posted for industry comment:
  – EACMS (Electronic Access Control or Monitoring Systems) Mixed Trust Authentication
  – Interactive Remote Access
  – Programmable Electronic Device
• Comment period ended February 6, 2015
• CIP V5 Transition Advisory Group working on post-comment revisions
CIP Version 5 Transition Update

• Top 15 Lessons Learned planned to be at least posted for industry comment by April 1, 2015
  – Lessons Learned plan posted on the NERC web site

• Next Lessons Learned expected to be posted for industry comment:
  – Generation Interconnection Point
  – Grouping BES Cyber Systems
  – Non-BA/non-TOP Control Centers
CIP Version 5 Transition Update

• Virtualization summit held by NERC
  – Brought together industry and key solution providers (Cisco and VMWare)
  – Looking to identify successful ways to deploy virtual environments (virtual machines, virtual LANs) within the CIP requirements
  – Virtualization Lesson Learned being developed by the V5 Transition Advisory Group with a late March target date to post for comment
  – The webinar was recorded and has been posted to the NERC web site
NERC-Sponsored Training

• **CIP Workshops and Curriculum** content being developed
  – Compilation of links and references to NERC and regional training, presentations, guidance, and other CIP V5 information

• **Small Group Advisory Training**
  – Three 3-day industry sessions scheduled in Atlanta:
    ▪ February 24-26, 2015
    ▪ March 24-26, 2015 (registration deadline 3/10/2015)
    ▪ April 21-23, 2015 (registration deadline 4/10/2015)
  – Registration links posted on **CIP V5 Event Calendar**
SPP Regional Outreach

- SPP RE and SPP RTO compliance staffs are collaborating on CIP V5 outreach
  - June “CIP Week” ([register here](#))
  - Webinars
  - Multi-entity outreach visits
  - One-on-one assistance visits

- Circulated an outreach survey to the SPP RE entities
  - Survey closed January 21, 2015; 57 respondents
  - Determined outreach needs by topic
  - Determined interest in site visits
### Outreach Survey Results

<table>
<thead>
<tr>
<th>Topic</th>
<th>Response percent</th>
<th>Response total</th>
</tr>
</thead>
<tbody>
<tr>
<td>Classifying BES Cyber Systems</td>
<td>55.56%</td>
<td>30</td>
</tr>
<tr>
<td>Grouping BES Cyber Systems</td>
<td>51.85%</td>
<td>28</td>
</tr>
<tr>
<td>Virtualization</td>
<td>35.19%</td>
<td>19</td>
</tr>
<tr>
<td>External Routable Connectivity</td>
<td>38.89%</td>
<td>21</td>
</tr>
<tr>
<td>Completing RSAWS (Reliability Standard Audit Worksheets)</td>
<td>37.04%</td>
<td>20</td>
</tr>
<tr>
<td>Evidence needed at audit</td>
<td>48.15%</td>
<td>26</td>
</tr>
<tr>
<td>Policy Template for CIP-003-5</td>
<td>44.44%</td>
<td>24</td>
</tr>
<tr>
<td>Document Template for CIP-004-5</td>
<td>33.33%</td>
<td>18</td>
</tr>
<tr>
<td>Document Template for CIP-006-5</td>
<td>33.33%</td>
<td>18</td>
</tr>
<tr>
<td>Document Template for CIP-010-1</td>
<td>37.04%</td>
<td>20</td>
</tr>
<tr>
<td>Programmable Electronic Devices</td>
<td>35.19%</td>
<td>19</td>
</tr>
<tr>
<td>Interactive Remote Access</td>
<td>40.74%</td>
<td>22</td>
</tr>
<tr>
<td>CIP Terms and Definitions</td>
<td>33.33%</td>
<td>18</td>
</tr>
<tr>
<td>System Baselining</td>
<td>44.44%</td>
<td>24</td>
</tr>
<tr>
<td>Other</td>
<td>12.96%</td>
<td>7</td>
</tr>
</tbody>
</table>

*Statistics based on 54 respondents*
CIP Standards Revisions

• Initial revisions, balloted as the “-X” standards, adopted by the NERC Board of Trustees November 13, 2014
  – CIP-003-6 – Security Management Controls
  – CIP-004-6 – Personnel & Training
  – CIP-006-6 – Physical Security of BES Cyber Systems
  – CIP-007-6 – System Security Management
  – CIP-009-6 – Recovery Plans for BES Cyber Systems
  – CIP-010-2 – Configuration Change Management and Vulnerability Assessments
  – CIP-011-2 – Information Protection
CIP Standards Revisions

• The initial revisions:
  – Removed Identify, Assess, and Correct Language from 17 requirements
  – Addressed the Communications Networks directives of FERC Order 791
    ▪ CIP-006-6 / Requirement Part 1.10: Physical protection of cabling and other non-programmable components of BES Cyber Systems existing outside of the PSP.
CIP Standards Revisions

• Remaining revisions, balloted as the “-7” standards, adopted by the NERC Board of Trustees February 12, 2015
  – CIP-003-7
  – CIP-004-7
  – CIP-007-7
  – CIP-010-3
  – CIP-011-3
CIP Standards Revisions

• The remaining revisions:
  – Clarified Cyber Security Plan requirements for Low Impact BES Cyber Systems
  – Clarified requirements for Transient Cyber Assets and Removable Media
  – Defined new terms
CIP Standards Revisions

• “-X” and “-7” changes merged into new Version 6
  – CIP-003-6 – Security Management Controls
  – CIP-004-6 – Personnel & Training
  – CIP-006-6 – Physical Security of BES Cyber Systems
  – CIP-007-6 – System Security Management
  – CIP-009-6 – Recovery Plans for BES Cyber Systems
  – CIP-010-2 – Configuration Change Management and Vulnerability Assessments
  – CIP-011-2 – Information Protection

• Submitted to FERC February 13, 2015
CIP-014-1 (Physical Security)

- Approved by FERC Order 802 on November 20, 2014
- Enforceable October 1, 2015
- Compliance milestones (latest date is Feb 16, 2017):
  - Initial Risk Assessment (IRA) complete on or before October 1, 2015
  - Assessment Verification (AV) = IRA + 90 calendar days
  - Assessment Modifications (AM) = AV + 60 calendar days
  - Control Center Notification (CCN) = AM + 7 calendar days
  - Security Plan (SP) = AM (or AV) + 120 calendar days
  - Security Plan Review (SPR) = SP + 90 calendar days
CIP-014 (Physical Security) Revisions

• Standard is being revised to address FERC Order 802 directives:
  – Remove the term “widespread” from CIP-014-1 or, alternatively, modify the standard to address Commission concerns
  – Responsive filing required six months after the effective date of Order 802 (due July 24, 2015)

• Risk Assessment and Third-Party Verifications guidance memorandum posted on the NERC web site
CIP Breakout Sessions

• Three CIP breakout sessions scheduled for this afternoon in the Auditorium
  1. 1:00 – 2:00: Change Control and Configuration Management
  2. 2:10 – 3:10: CIP V5 Lessons Learned and FAQ Discussion
  3. 3:40 – 4:40: Open Q&A

• We plan to keep the WebEx and conference call open due to popular demand
Helpful Resources

• **NERC Website Links:**
  
  – [CIP V5 Transition Home Page](#)
    
    ▪ [CIP V5 Standards and Implementation Plan](#)
    
    ▪ [CIP V5 Transition Guidance](#)
    
    ▪ [CIP V5 Transition Study Lessons Learned](#)
  
  – [Project 2014-04 (Physical Security)](#)
    
    ▪ [CIP-014-1](#)
    
    ▪ [CIP-014-1 Implementation Plan](#)
    
    ▪ [CIP-014 Revisions SAR](#)
Helpful Resources

• SPP RE Website: CIP V5 Outreach
  – Identifying BES Cyber Systems SPP RE Webinar Updated 10-30-14
  – CIP V5 Transition Guidance SPP RE webinar- 2014-09-04
  – CIP_V5_SPP RE Hands-On Training Materials March_2014
SPP RE CIP Team

- **Kevin Perry**, Director of Critical Infrastructure Protection  
  (501) 614-3251
- **Shon Austin**, Lead Compliance Specialist-CIP  
  (501) 614-3273
- **Steven Keller**, Lead Compliance Specialist-CIP  
  (501) 688-1633
- **Jeremy Withers**, Senior Compliance Specialist-CIP  
  (501) 688-1676
- **Robert Vaughn**, Compliance Specialist II-CIP  
  (501) 482-2301
ERO Enterprise Risk-based Compliance Monitoring

SPPRE 2015 Spring Workshop
Adina Mineo, Compliance Assurance Manager, NERC
• Risk-based compliance update
• Implementation of Inherent Risk Assessment (IRA) and Internal Control Evaluation (ICE) Guides and examples
• Review of Frequently asked questions (FAQs)
2014 Accomplishments

- All design documents completed and published
- Trained 100% of Regional Entities on performance
- Extensive stakeholder collaboration and outreach
- FERC filing
• The design of the risk-based compliance monitoring and enforcement program (CMEP) is completed
  ▪ Enhanced, more efficient use of ERO Enterprise and industry resources
  ▪ Comprehensive collaboration and outreach to promote stakeholder understanding
  ▪ Organization and publication of resource materials on NERC website
• 2015 is an implementation year
• Oversight, training, and continued guidance through 2015 support consistency of process
• NERC communications will reference risk-based compliance monitoring and enforcement instead of RAI going forward
• RAI page on NERC.com will remain in place during 2015 to ensure availability of information
  ▪ Content will be duplicated in Compliance and Enforcement pages, which are being redesigned for usability
  ▪ New information will continue to be highlighted in weekly bulletins and monthly newsletters
Implementation of Risk-based CMEP

ERO Enterprise Staff Training

Continued Outreach

2015 Implementation

Oversight

Metrics
• 2014 included specific, role-based training on Inherent Risk Assessment (IRA) and Internal Control Evaluation (ICE)
• Multi-regional and face-to-face training
• 100% Regional Entity participation
2015 ERO Enterprise Staff Training

- 2015 training focuses on consistent implementation:
  - Continuous through implementation
  - Train on identified competencies
  - Tailored to “performance” role for each design component
  - Compliance monitoring and enforcement staff

- Use of training management system
  - Track training records and role attributes by individual
  - Facilitates reporting

- Tabletop exercise on small-entity internal controls
Continued Outreach

- Webinar outreach series on Reliability Standards associated with Risk Elements
- Stakeholder workshops
  - March 5, 2015 (Atlanta, GA)
  - Fall 2015 (date/location TBA)
- Semi-annual Standards and Compliance workshops
- Participation in stakeholder, trades, and forum events
- Collaborate with advisory group to focus outreach effectively
• Goals of oversight:
  ▪ Support successful implementation
  ▪ Consistency
  ▪ Conceptual alignment and consistency with design documents
  ▪ Identify best practices and opportunities
  ▪ Adherence to the Rules of Procedure and delegation agreements
• Oversight approach:
  ▪ Review of processes and procedure documents to assess consistency with risk-based CMEP design
  ▪ Sampling of activities related to performance of specific components of the risk-based CMEP design
  ▪ Feedback and recommendations to Regional Entities for improvement and training
• Concurrent with implementation (i.e., it is already underway)
• Results in regular feedback to Regional Entities
• Publish report assessing consistency of Regional Entity compliance monitoring by end of 2015
• Publish annual ERO Enterprise risk-based CMEP report in Q1 2016
Compliance Assurance Oversight

• Phase I
  ▪ Q1-Q2 of 2015
  ▪ Process and document reviews of each region to establish conceptual consistency and to identify and resolve any nonconformance to the risk-based CMEP’s design
  ▪ Feedback to the Regional Entity with recommendations

• Phase II
  ▪ Q3 2015 and beyond
  ▪ Evaluation of how risk-based compliance monitoring concepts are used (including determinations and application)
  ▪ Focus on samples of compliance monitoring work
  ▪ Review of performance of the compliance monitoring work
  ▪ Feedback to the Regional Entity with recommendations
• Developed with input from stakeholder advisory group
• Effectiveness criteria being developed with NERC CCC
• Will be reported quarterly and in support of benchmarking results in 2015
• Intended to support success factors:
  ▪ ERO Enterprise staff competency (competency and perception)
  ▪ Information and outreach
  ▪ Consistency
  ▪ Regulator trust
  ▪ Balanced transparency
  ▪ Metrics identified
  ▪ Recognized value
Questions and Answers
Session Objectives

- Cite the purpose and components of the Risk-based Compliance Oversight Framework (Framework).
- Discussion on industry frequently asked questions—“How does risk-based compliance impact me as a registered entity?”
Framework

Risk Elements

- Registered Entity Functions
- ERO & Regional Characteristics
- Events
- RISC

IRA

Inherent Risk Assessment

ICE

Internal Controls Evaluation

CMEP Tools

Scope and Focus for Entities not participating in ICE

Focus

Entity Compliance Oversight Plan
• Identify areas of focus and effort needed to monitor compliance with Reliability Standards
• Input to Internal Control Evaluation module
• Develop a draft risk-based Region-specific compliance oversight plan
  ▪ Consists of areas of focus, including Reliability Standards and Requirements, timing, and possible CMEP tool
• Risk Elements Guide details process used to identify and prioritize Enterprise-wide risks

• Annual CMEP Implementation Plan is mechanism for delivering risk element results
  ▪ ERO Enterprise risks to the reliability of the BPS for compliance monitoring.
  ▪ Associated Reliability Standards and Requirements mapped to the reliability risks.
  ▪ Regional risk considerations.

• Understanding the entity
Transmission Owner Comparisons

Large Transmission Owner
- Interconnects
  - 150 interconnection locations with 12 different entities
- Owns following BES transmission lines:
  - 2200 miles of 115 kV
  - 400 miles of 161 kV
  - 420 miles of 230 kV
  - 250 miles of 500 kV
- Winter Peak load: 7,000 MW
- Summer Peak load: 9,200 MW
- Owns four SPS
- Owns four elements of an IROL flowgate
- UFLS installed at 80 busses capable of shedding 3000 MW
- Owns five UVLS schemes

Small Transmission Owner
- Interconnects
  - Six locations with 6 entities
- Owns ten BES transmission lines:
  - 10 miles of 115 kV
  - 100 miles of 161 kV
  - 20 miles of 230 kV transmission.
- Peak load is 500 MW.
- Does not own SPS
- Does not own any elements of an IROL flowgate
- Has not been assigned any UFLS responsibilities
- Does not own any UVLS
Standards and requirements related to the TO function.

<table>
<thead>
<tr>
<th>Entity</th>
<th>Number of Standards in Monitoring Scope</th>
<th>Number of Standards in Common</th>
<th>Number of Requirements in Monitoring Scope</th>
<th>Number of Requirements in Common</th>
</tr>
</thead>
<tbody>
<tr>
<td>Large</td>
<td>12</td>
<td>5</td>
<td>19</td>
<td>5</td>
</tr>
<tr>
<td>Small</td>
<td>5</td>
<td>5</td>
<td>8</td>
<td>5</td>
</tr>
</tbody>
</table>
## Example Requirements

<table>
<thead>
<tr>
<th>Requirement</th>
<th>In Scope for Large TO</th>
<th>In Scope for Small TO</th>
<th>Rationale</th>
</tr>
</thead>
<tbody>
<tr>
<td>FAC-008-3 R3</td>
<td>X</td>
<td>X</td>
<td>A review to ensure an entity that owns BES transmission has an adequate facility ratings methodology is appropriate.</td>
</tr>
<tr>
<td>PRC-004-2.1a R1</td>
<td>X</td>
<td></td>
<td>Review of completion of CAPs is appropriate for the larger entity since it has reported 50+ misoperations over last three years and owns over 3,000 miles of BES transmission.</td>
</tr>
<tr>
<td>PRC-006-1 R9</td>
<td>X</td>
<td></td>
<td>UFLS operations could impact BPS reliability and should be monitored. Smaller entity has not been assigned UFLS responsibilities.</td>
</tr>
<tr>
<td>PRC-017-0 R2</td>
<td>X</td>
<td></td>
<td>Review of SPS maintenance and testing is appropriate since larger entity owns 4 SPS and over 3,000 miles of BES transmission. Smaller entity does not own any SPS.</td>
</tr>
</tbody>
</table>
• Regional Entities will collaborate and hold discussions throughout the IRA process
  ▪ Collaboration will help ensure IRA results include appropriate and sufficient information
  ▪ Regional Entities are owners of the IRA process
• Results will include risk areas identified, associated Reliability Standards and Requirements, and preliminary oversight plan
  ▪ IRA results are an opportunity to describe a risk and the registered entity’s relationship to that risk. It is the Region’s assessment and the registered entity should understand the process and the results.
  ▪ Presenting the results to the registered entity allows for clarity and transparency
• Considerations
  ▪ Levels of risk and depth needed to obtain reasonable assurance for each area of focus
  ▪ Monitoring methods to be employed and which standards/requirements are in scope for each
  ▪ Timing of compliance monitoring activities
  ▪ Available resources
2015 IRA Implementation

- Regional processes should follow IRA Guide
- Varying levels of Regional implementation throughout 2015
- IRAs expected to be completed for all 3-year audits scheduled in 2015
  - IRA will initially drive audit scope
- IRA revisions process should include lessons learned
Long-term IRA Implementation

• IRAs will help drive compliance monitoring plans for all entities, including 3-year cycle entities
• Consistency in approach is necessary – from both a transparency and oversight perspective
• Regional Entities should develop plans to complete all registered entity IRAs
• Focus compliance monitoring efforts
• Evaluate registered entity controls for identified risks and associated Reliability Standards and Requirements identified in IRA
• Help appropriately scope a compliance engagement
ICE Scope Considerations

• Collaborative engagement with entity to finalize scope of ICE
  ▪ ICE may be limited to only certain or some controls
    o Up to registered entity to identify which controls to provide
    o Controls may be specific to a Standard, requirement, or process
  ▪ ICE may be tied to parts of an IRA, all of IRA, or not an IRA
    o For example: CIP-002
    o Focused on a certain function or business unit
  ▪ Scope of ICE is not dependent on entity size

• ICE activities may occur in parallel with IRA activities

• Using the work of others
What is an Internal Control?

Internal Controls as defined by the GAO:

An integral component of an organization’s management that provides reasonable assurance that the following objectives are being achieved:

• effectiveness and efficiency of operations,
• reliability of financial reporting, and
• compliance with applicable laws and regulations.

Taken from United States General Accounting Office Standards for Internal Control in the Federal Government

• Provide accountability to employees, management, and regulators

• Encourage sound management practices
  • Reduce risks to reliability
  • Manage resources
  • Safeguard assets
  • Promote operational efficiencies
  • Coordinate cross-functional policies and procedures

• Obtain assurance of effective and efficiency of operations and compliance with Reliability Assurance
Nature of Internal Controls

• Internal controls can vary in nature and complexity
  ▪ Electronic controls, such as employee ID cards, fences, locks, VPN, or fireproof files
  ▪ Independent verification of processes deliverables
  ▪ Authorizations of employee timecards
Basic Types of Controls

- Preventative
  - Aimed at preventing any errors or irregularities from occurring which may have negative effects
  - **Example:** Documented process requiring development and maintenance of training schedule

- Detective
  - Designed to find out and discover the different errors or irregularities which may have occurred
  - **Example:** Documented process requiring periodic review to identify any required training not completed as scheduled, as well as training not completed per reliability standard requirements
    - Quarterly review of completed training records to identify individuals who have not completed training by the required deadline
    - Documentation and utilization of an event review and root cause analysis process to determine cause and effects surrounding an unwanted event
• Corrective
  ▪ Corrective controls restore the system or process back to the state prior to a harmful event
  ▪ **Example 1:** Automatic Voltage Regulator
  ▪ **Example 2:** Corrective controls restore the system or process back to the state prior to a harmful event. For example, a business may implement a full restoration of a system from backup tapes after evidence is found that someone has improperly altered the payment data
Levels of Internal Controls

- **CIP Examples**
  - Entity Level Control to ensure operations and compliance staff are consistent
    - Management establishes a formal policy to review critical processes and procedures to be conducted jointly by Operations and Compliance Staff on a periodic basis
  - Activity Level Control to ensure backup media is periodically tested per CIP-009 R5
    - Automated backups, verification by personnel, backups tested

- **O&P Examples**
  - Entity Level Control to ensure testing records are properly maintained
    - Require personnel which creates any compliance records (for both CIP and O&P such as testing records or operating plans) to maintain the data in a central location
  - Activity Level Control to ensure relay test records are maintained
    - Use relay test records retention software to allow staff to roll back changes in case of adverse effects
• Internal controls related to COM-002
  ▪ Prevent control involved Registered Entity using three-part communication for routine communications (policy for all communications)
  ▪ Preventive control involves random review of operator communications, followed by feedback and corrective actions
  ▪ Detective control involves complete review of any situation in which a directive may be issued

• Conclusion was that registered entity will identify and address issues timely
  ▪ Reviewed evidence to ensure random reviews were conducted and reviewed evidence that entity conducted reviews of situations were they believed a directive may be issued and the results of the review

• Based on results of internal control testing, Standard was not tested directly
Example No. 2: CIP-007 R3

• CIP Controls Example
  ▪ Risk Area = Configuration Management
  ▪ CIP-007 R3
  ▪ Patches are tested internally in association with a change request
  ▪ Uses automated tool to automatically track patches were applicable, otherwise has manual process in place
  ▪ Uses SharePoint to ensure patch management processes are being followed
Example No. 2: CI P-007 R3

Patch Management

- Asset identified
- Applications identified
- Patch locations identified
- Patch tracking planned
- Patches tracked
- Patches identified
- Patches evaluated
- Patches tested
- Patches installed
- Patches installation documented
ICE Impact on Registered Entities

- Small, low risk registered entities may require limited internal control evaluation
- There is no expectation to create an internal control for each and every Requirement (Some Standards and Requirements may be controls)
- ICE does not intend to identify possible noncompliance and a lack of or weak internal controls does not indicate possible noncompliance
- ICE Guide does not require new processes or new documentation to be developed by a registered entity, though some level of documentation may be needed to illustrate design and effectiveness of control
• Evaluation factors to review and consider reliance
  ▪ Independence
  ▪ Qualifications
  ▪ Quality of work papers
  ▪ Methodology
  ▪ Retesting
  ▪ Acceptance
Perform a walkthrough of key controls identified

- Trace the controls and related processes and procedures to understand whether it is designed to work effectively (eliminate exposure to risk)
- Consider sampling approach. Is the sample relevant?
- Stacking of evidence
- Information credibility
- Information sufficiency
Verifying Control Information - Sufficiency

- Is the information validated by more than one source?
- Is sufficient information about the controls operation available?
  - Potential impact on the reliability of the BES
  - Frequency of the control
  - Monitoring the control
  - Functions (walk-through the control)
  - Entity Size
  - Subject to management override
  - Automated or manual
  - Preventative, corrective, or detective
Verifying Control Information - Credibility/ Timeliness

- Is the registered entity’s current control information on file?
- Is any of the control information on file outdated?
- Is there any incomplete or missing control information?
Control Characteristics to Consider

• Factors to consider
  ▪ Manual vs. automated controls
  ▪ Preventive vs. detective
  ▪ Can controls be overridden
  ▪ Management oversight
  ▪ Conflict of interest
  ▪ Segregation of duties
  ▪ How well are employees trained
  ▪ Are responsibilities for controls assigned
• Reflect how ICE impacts monitoring activity from example
• Compliance monitoring activities may become more frequent, but less intrusive
  ▪ Shift from large, infrequent audits to “continuous” monitoring
• Focused scope for monitoring places emphasis on areas that present highest risk to reliability of the BES
• Regions to make better use of all the tools provided by the CMEP, not just audits
Frequently Asked Questions

• How does risk-based compliance monitoring impact a registered entity?
  ▪ Voluntary aspects
  ▪ Timing
  ▪ Benefits
  ▪ Preparation for ICE
  ▪ Expectation of ICE documentation
  ▪ “FERC 13” Culture of Compliance
  ▪ MRRE
  ▪ NERC Oversight
• Voluntary aspects
  - ICE is voluntary, IRA is part of the ERO Enterprise process for determining how to monitor risk
  - ICE only helps focus regional compliance monitoring activities for identified risks (from IRA)
  - ICE does not evaluate compliance with Reliability Standards

• Timing
  - Short-term, 2015, Regions are prioritizing IRAs starting with audit schedule
  - All registered entities will have an IRA, but it is depending on regional timing, risk, and resources

• Benefits
  - Focus on reliability benefit versus compliance effort and reduced administrative burdens
  - Assurance of effective and efficiency of operations and compliance with Reliability Assurance
• Preparation for ICE
  ▪ Begin reviewing Risk Elements and internally evaluating risks posed to the BPS
  ▪ Understand current processes in place that may be internal controls
    o What record is produced by the internal control?
    o What results are expected/evident?
    o How are the records managed? Easily retrievable?
    o How effective is the internal control?
    o How does monitoring occur? Are there tertiary monitoring aspects?
    o What harm can occur if the internal control fails?
    o Why does the internal control exist? How was the internal control generated?
• Expectations for IRA and ICE
  - IRA and ICE is a coordinated effort
  - Registered entities will see IRA results and have information explaining IRA results
  - There is no expectation to create an internal control for each and every Requirement (Some Standards and Requirements may be controls)
  - Some documentation may be needed to demonstrate design and effectiveness of control

“FERC 13 Questions” on Culture of Compliance
  - Action item by NERC and Regional Entities to determine purpose, obligation, and process
  - Existing process will be followed and questions asked during IRA process
• Coordinated Oversight (MRRE)
  ▪ Regional Entities are coordinating activities for IRA and ICE for entities registered in multiple regions
  ▪ Notifications to MRREs have begun to determine next steps for compliance activities

• Ongoing Education and Outreach
  ▪ NERC and the REs plan to continue outreach and education on lessons learned and sharing of best practices
Questions and Answers
Protection System

Part Deux*

*A superficial, unnecessary, or overly bad sequel. Usually the second in the series though not always (see CIP). Adding the phrase to a title is similar to adding the "electric boogaloo. Examples include: “BAL-006-2," “MOD-025-2," “NERC Functional Model Version 2," “SPP PC UFLS Plan Rev 2," etc.**

** This is not the case.
Agenda

• Review Cleco Transition to PRC-005-2
  – What Changed?
  – What could we miss?
• Reliability Assurance Initiative
  – Internal Controls
Transition

• From a “Maintenance and Testing Program”

• To a maintenance program which includes at least one of the following activities:
  
  ➢ Verify  
  ➢ Monitor  
  ➢ Test  
  ➢ Inspect  
  ➢ Calibrate
Activities include:

- Verify: Determine that the component is functioning correctly.
- Monitor: Observe the routine in-service operation of the component.
- Test: Apply signals to a component to observe functional performance or output behavior, or diagnose problems.
- Inspect: Examine for signs of component failure, reduce performance or degradation.
- Calibrate: Adjust the operating threshold or measurement accuracy of a measuring element to meet the intended performance requirement.
Evidence

• See Protection System Maintenance and Testing Program

190 READ R$, S
200 IF R$ = “END OF FILE” THEN 340
210 IF X = PROTECTION SYSTEM THEN 212
211 GOTO 215
212 VERIFY, MONITOR, TEST, INSPECT, CALIBRATE
213 X = X+1
214 GOTO 210
215 READ R$, S
216 GOTO 200
340 PRINT “FINI”
350 END
NERC Transition

• See the mapping document at:

<table>
<thead>
<tr>
<th>Version 1</th>
<th>Version 2</th>
</tr>
</thead>
<tbody>
<tr>
<td>Batteries &amp; Chargers</td>
<td>Batteries &amp; Chargers</td>
</tr>
<tr>
<td>Current Transformers</td>
<td>Current Transformers</td>
</tr>
<tr>
<td>Potential Transformers</td>
<td>Potential Transformers</td>
</tr>
<tr>
<td>Carrier systems</td>
<td>Carrier systems</td>
</tr>
<tr>
<td>Wavetraps</td>
<td>Wavetraps</td>
</tr>
<tr>
<td>UF relays</td>
<td>UF relays</td>
</tr>
<tr>
<td>Protection Relays</td>
<td>Protection Relays</td>
</tr>
<tr>
<td>Special Protection Schemes</td>
<td>Remedial Action Systems</td>
</tr>
<tr>
<td>Protection Functional test (trip checks)</td>
<td>Protection Functional test (trip checks)</td>
</tr>
<tr>
<td></td>
<td>UF Functional test</td>
</tr>
<tr>
<td></td>
<td>Alarms or monitoring</td>
</tr>
</tbody>
</table>
Cleco’s Program

• Our Program is strictly “Time-Based”
<table>
<thead>
<tr>
<th>Component Attribute</th>
<th>Maximum Interval for Unmonitored</th>
<th>Maximum Interval for Monitored</th>
</tr>
</thead>
<tbody>
<tr>
<td>Protective Relay</td>
<td>6 years</td>
<td>12 years</td>
</tr>
<tr>
<td>Communications system</td>
<td>4 months &amp; 6 years</td>
<td>12 years</td>
</tr>
<tr>
<td>Voltage &amp; current sensing devices</td>
<td>12 years</td>
<td>None</td>
</tr>
<tr>
<td>Protection System DC supply</td>
<td>4 months &amp; 18 months</td>
<td>None</td>
</tr>
<tr>
<td>Control Circuitry</td>
<td>6 or 12 years</td>
<td>None</td>
</tr>
<tr>
<td>Alarm Path</td>
<td>12 years</td>
<td>None</td>
</tr>
<tr>
<td>UFLS/UVLS</td>
<td>6 years</td>
<td>12 years</td>
</tr>
</tbody>
</table>
Cleco Intervals

• Cleco’s maximum intervals did change due to monitoring.
What didn’t change for relays.

- **Protective Relays**
  - **Verify** that settings are as specified.
    - include statement in test
  - **Test and calibrate**
  - **Verify** operation of inputs & outputs
  - **Verify** alarm path
Cleco changes for relays

• For protective relays:
  – Verify acceptable measurement of power system input values
  – Microprocessor: run software comparison report for settings comparison
What didn’t change for communication systems.

• Carrier & Wavetraps
  – Verify that the communications systems meets performance criteria pertinent to the communications technology applied.
Cleco changes for communication systems

• Carrier & Wavetraps:
  – Verify automated testing for the presence of the channel function and alarming for the loss of function
  – Verify operation of the communications system inputs and outputs that are essential to proper functioning of the Protection System.
What didn’t change for voltage & current sensing devices.

• PT & CT
  – Verify that current and voltage signal values are provided to the protective relays.
What changed for voltage & current sensing devices.

• PT & CT
  – Nothing
What didn’t change for batteries

• **Batteries**
  – **Verify** station dc supply voltage
  – **Inspect** Electrolyte level
  – **Inspect** for unintentional grounds
  – Replace valve regulated type batteries
Cleco changes for batteries

• **Batteries vented lead acid:**
  
  – Quarterly **inspection** now every 4 calendar months
  
  – Annual **Inspection** must be done within 18 calendar months
  
  – **Inspect** physical condition of the battery rack
  
  – Load **test** interval increased to 6 years
Cleco changes for batteries cont.

- **Batteries valve regulated:**
  - Quarterly inspection now every 4 calendar months
  - Inspect condition of all cells every 6 calendar months
  - Annual Inspection must be done within 18 calendar months
  - Inspect physical condition of the battery rack
  - Replace interval changed to 3 years
What didn’t change for control circuitry

• Control Circuitry
  – Verify that each trip coil is able to operate...
  – Verify electrical operation of electromechanical lockout devices
Cleco changes for control circuitry

• Functional (control circuitry) trip checks:
  – Interval changed to 6 years

• Alarm Paths & Monitoring:
  – Verify alarm paths are reported within 24 hours of detection to a location where corrective action can be initiated.
What didn’t change for UFLS

• UFLS
  – Verify that settings are as specified
  – Test and calibrate
  – Verify operation of relay inputs and outputs
Cleco changes for UFLS

- **UFLS Relays:**
  - Verify acceptable measurement of power system input values

- **UFLS DC supply for non-BES devices:**
  - Verify dc supply voltage at the UFLS relay.

- **UFLS functional trip checks:**
  - Verify all UFLS paths of the trip circuit
What could we miss!

• Unresolved Maintenance Issues:
  – A deficiency identified during a maintenance activity that causes the component to not meet the intended performance, cannot be corrected during the maintenance interval, and requires follow-up corrective action.

  – Cleco will document within the maintenance database the corrective action plan. Included will be a description of the problem, who was notified of the problem (System Operations, Generation Operations, or operating personnel at the plant), and a description of the corrective action to resolve the issue.
Questions
Reliability Assurance Initiative
Internal Controls for PRC-005

• Cleco has recently added personnel from our internal audit group to develop internal controls for all standards.

• We had controls but they were not necessarily documented.

• Goal is to have controls in place which will prevent us from having a compliance violation.
Types of Controls

• **Preventive:** Annually, the GMs approve the Protection System Maintenance and Testing Program.
  
  – *Expected Documentation:* Approval emails or signoff sheet
  
  – *Test to be performed:* Prior to year end document the approval.
Types of Controls cont.

• Preventive: Monthly, evidence prompter sends email to maintenance managers requesting status update of battery inspections.
  – Expected Documentation: Evidence prompter emails. Status update email from each manager
  – Test to be performed: Obtain and document a copy of the email generated by evidence prompter and manager update email.
Types of Controls cont.

• **Detective**: Weekly, the network folder is verified to store all database maintenance orders processed during the prior week.
  
  – **Expected Documentation**: Weekly spreadsheet with comparison results. If applicable, evidence requesting corrections.
  
  – **Test to be performed**: Obtain copy of spreadsheet
• Detective & Corrective: Quarterly, run report in maintenance database to determine if any equipment is scheduled to be completed by the end of the year.
  – Expected Documentation: Quarterly reports for component types.
  – Test to be performed: Obtain copy of report
Take Away

• As a field engineer, it is important to test the Protection System components to make sure the grid is reliable.

• As a compliance person, it is important to test our program to make sure all aspects of the standards are included in the program; all aspects of our program are completed and our program is functioning as expected.
QUESTIONS
Contact

• Louis C. Guidry, PE

• [louis.guidry@cleco.com](mailto:louis.guidry@cleco.com)

• cell 318-308-9121

• work 318-484-7495

Copies of Cleco’s Protection System Maintenance and Testing Program are available upon request.
SPP RE General Manager’s Report

2015 Spring Workshop
Little Rock, Arkansas

Ron Ciesiel
SPP RE General Manager
INDICATORS OF SUCCESS
Violations by Year

![Graph showing violations by year with projected data for 2014. The graph compares ERO Total and SPP RE violations over the years 2009 to 2014.]}
Event Reporting and Analysis

- 30 Events Reported in SPP RE during 2014
  - 3 Category 2 [out of 5 categories]
  - 13 Category 1
  - 14 Reported but did not reach minimum threshold

- Excellent operational performance overall
- Excellent participation and response by the Registered Entities to the requirements of the program
Vegetation Management

• NERC 4Q 2014 Vegetation Management Report
  – No reportable contacts in SPP RE footprint
  – 7th consecutive quarter with no reportable contacts

• Prior to 1Q 2013 contact achieved 10 consecutive quarters with no reportable contacts
SPP RE Misoperation Report as of 3Q 2014

Correct Operations
Rolling 4 Quarter Average

<table>
<thead>
<tr>
<th>Quarter</th>
<th>Correct Operations</th>
<th>Rolling 4 Quarter Average</th>
</tr>
</thead>
<tbody>
<tr>
<td>Q1-11</td>
<td>85.2%</td>
<td></td>
</tr>
<tr>
<td>Q2-11</td>
<td>89.8%</td>
<td></td>
</tr>
<tr>
<td>Q3-11</td>
<td>88.8%</td>
<td></td>
</tr>
<tr>
<td>Q4-11</td>
<td>82.9%</td>
<td></td>
</tr>
<tr>
<td>Q1-12</td>
<td>91.2%</td>
<td></td>
</tr>
<tr>
<td>Q2-12</td>
<td>91.8%</td>
<td></td>
</tr>
<tr>
<td>Q3-12</td>
<td>89.3%</td>
<td></td>
</tr>
<tr>
<td>Q4-12</td>
<td>84.6%</td>
<td></td>
</tr>
<tr>
<td>Q1-13</td>
<td>85.7%</td>
<td></td>
</tr>
<tr>
<td>Q2-13</td>
<td>87.2%</td>
<td></td>
</tr>
<tr>
<td>Q3-13</td>
<td>86.3%</td>
<td></td>
</tr>
<tr>
<td>Q4-13</td>
<td>88.3%</td>
<td></td>
</tr>
<tr>
<td>Q1-14</td>
<td>92.3%</td>
<td></td>
</tr>
<tr>
<td>Q2-14</td>
<td>91.8%</td>
<td></td>
</tr>
<tr>
<td>Q3-14</td>
<td>86.0%</td>
<td></td>
</tr>
</tbody>
</table>
Operation/Misoperation Comparison

![Graph showing operation and misoperation comparison from Q1-11 to Q3-14. The graph includes bars for operations and misoperations, with rolling 4 quarter averages indicated by lines.](image-url)
Alerts/Guidance/Surveys

• Facilities Ratings Alert
  – Rolling towards completion
  – All SPP RE entities are either finished or have an approved extension

• Winterization/Southwest Blackout Guidance
  – No major issues since winter/summer of 2011
  – No new Standards contemplated

• Surveys in lieu of mandatory standards
  – Gauges responsiveness to Guidance documents
  – Currently requesting responses for assistance in Clean Power Plant assessment
## Most Violated Standards

Based on rolling 12 months through 1/31/15 [Represents ~ 88% of total violations]

<table>
<thead>
<tr>
<th>SPP RE Rank</th>
<th>NERC 12 Month Rank *</th>
<th>Standard</th>
<th>Description</th>
<th>Number of Violations</th>
<th>Risk Factor</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>1</td>
<td>CIP-007</td>
<td>Systems Security Management</td>
<td>28</td>
<td>Med./Lower</td>
</tr>
<tr>
<td>2</td>
<td>3</td>
<td>CIP-005</td>
<td>Electronic Security Perimeters</td>
<td>15</td>
<td>Med./Lower</td>
</tr>
<tr>
<td>3</td>
<td>2</td>
<td>CIP-006</td>
<td>Physical Security - Critical Cyber Assets</td>
<td>13</td>
<td>Med./Lower</td>
</tr>
<tr>
<td>4</td>
<td>6</td>
<td>CIP-003</td>
<td>Security Management Controls</td>
<td>12</td>
<td>Med./Lower</td>
</tr>
<tr>
<td>5</td>
<td>10</td>
<td>FAC-008</td>
<td>Facility Ratings (includes FAC-009)</td>
<td>11</td>
<td>Med./Lower</td>
</tr>
<tr>
<td>6</td>
<td>7</td>
<td>CIP-002</td>
<td>Critical Cyber Asset Identification</td>
<td>8</td>
<td>High/Lower</td>
</tr>
<tr>
<td>7</td>
<td>4</td>
<td>CIP-004</td>
<td>Personnel &amp; Training</td>
<td>8</td>
<td>Med./Lower</td>
</tr>
<tr>
<td>8</td>
<td>8</td>
<td>VAR-002</td>
<td>Network Voltage Schedules</td>
<td>6</td>
<td>Med./Lower</td>
</tr>
<tr>
<td>9</td>
<td>5</td>
<td>PRC-005</td>
<td>Protection System Maintenance</td>
<td>4</td>
<td>High/Lower</td>
</tr>
<tr>
<td>10</td>
<td>**</td>
<td>TOP-002</td>
<td>Normal Operations Planning</td>
<td>2</td>
<td>Med./Lower</td>
</tr>
</tbody>
</table>

* NERC as of June 30, 2014
** Not in NERC Rolling 12 month Top Ten
INDICATORS OF CHANGE
Changing the Mix of Entities and Facilities

- BES Definition Update – Summer of 2014
- Registration Overhaul – expected 2015
  - Elimination of LSE, PSE, and IA functions
  - Raise threshold for DP participation
- Registration Overhaul – Part 2 – expected 2016
  - Technical studies to determine other thresholds or application of standards
Changes to Oversight

• More discretion given to Regional Entities concerning oversight plans based on risk analysis
  – Removes one-size fits all
  – Introduces more flexible audit planning
  – Provides opportunity for more review of Registered Entity’s internal monitoring processes
    ▪ Allows for self-logging of violations

• More discretion given to Regional Entities by removing zero tolerance mandate
  – Increases use of professional judgment based on materiality
Changes to Enforcement

• More discretion concerning disposition of reported violations
  – Added ‘Compliance Exception’ status at end of 2014
  – Impact of prior violations reviewed in historical context
    [Statute of Limitations]
INDICATORS OF CONTINUING IMPROVEMENT OPPORTUNITIES
Causes of Misoperations  3Q 2012-3Q 2014
Misoperations by Voltage
Misoperations by Type

- Unnecessary Trip during fault
- Unnecessary Trip other than fault
- Failure to Trip
- Slow Trip
- Still Under Review
# Most Violated Standards

Based on rolling 12 months through 1/31/15 [Represents ~ 88% of total violations]

<table>
<thead>
<tr>
<th>SPP RE Rank</th>
<th>NERC 12 Month Rank *</th>
<th>Standard</th>
<th>Description</th>
<th>Number of Violations</th>
<th>Risk Factor</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>1</td>
<td>CIP-007</td>
<td>Systems Security Management</td>
<td>28</td>
<td>Med./Lower</td>
</tr>
<tr>
<td>2</td>
<td>3</td>
<td>CIP-005</td>
<td>Electronic Security Perimeters</td>
<td>15</td>
<td>Med./Lower</td>
</tr>
<tr>
<td>3</td>
<td>2</td>
<td>CIP-006</td>
<td>Physical Security - Critical Cyber Assets</td>
<td>13</td>
<td>Med./Lower</td>
</tr>
<tr>
<td>4</td>
<td>6</td>
<td>CIP-003</td>
<td>Security Management Controls</td>
<td>12</td>
<td>Med./Lower</td>
</tr>
<tr>
<td>5</td>
<td>10</td>
<td>FAC-008</td>
<td>Facility Ratings (includes FAC-009)</td>
<td>11</td>
<td>Med./Lower</td>
</tr>
<tr>
<td>6</td>
<td>7</td>
<td>CIP-002</td>
<td>Critical Cyber Asset Identification</td>
<td>8</td>
<td>High/Lower</td>
</tr>
<tr>
<td>7</td>
<td>4</td>
<td>CIP-004</td>
<td>Personnel &amp; Training</td>
<td>8</td>
<td>Med./Lower</td>
</tr>
<tr>
<td>8</td>
<td>8</td>
<td>VAR-002</td>
<td>Network Voltage Schedules</td>
<td>6</td>
<td>Med./Lower</td>
</tr>
<tr>
<td>9</td>
<td>5</td>
<td>PRC-005</td>
<td>Protection System Maintenance</td>
<td>4</td>
<td>High/Lower</td>
</tr>
<tr>
<td>10</td>
<td>**</td>
<td>TOP-002</td>
<td>Normal Operations Planning</td>
<td>2</td>
<td>Med./Lower</td>
</tr>
</tbody>
</table>

* NERC as of June 30, 2014
** Not in NERC Rolling 12 month Top Ten
EMS/SCADA Related Events

• EMS/SCADA related events make up 33%+ of open events at the NERC level
  – Similar statistics @ SPP RE

• Not enough historical information to determine if this issue is rising or is more visible because other events are dropping in number

• NERC level taskforce has been formed to review and recommend
Mike Gabriel
Director, Critical Infrastructure Compliance
EthosEnergy Group – Power Plant Services
mike.gabriel@ethosenergygroup.com

SPP Spring Workshop
Little Rock, Arkansas
March 19-21, 2014
# Who is EthosEnergy?

## Wood Group

- Power Plant Services
- Oil & Gas Industrial Services
- Power Solutions (EPC)
- Construction Site Services
- Aero, Steam & Union Field Services
- Wood Group P&W Joint Venture

## Siemens

- Gas Turbine OEM (Fiat / Westinghouse)
- Gas Turbine Services
- Steam Turbine Services
- Generator Services
- Compressor Services
Agenda

- NAGF Overview
- Current GO / GOP Issues
- Info Sharing: Lessons Learned
The NAGF mission is to promote the safe, reliable operation of the generator segment of the bulk electric system through generator owner and operator collaboration with grid operators and regulators.
NAGF – Strategic Goals

➢ Grow the NAGF to be the premier organization dedicated to generator reliability issues

➢ Foster relationships with regulators and advocacy groups to provide avenues to educate and collaborate on the needs of NAGF members

➢ Promote effective information exchange and learning opportunities for and between members
NAGF – Current Status

- Completed incorporation as North American Generator Forum, Inc., a tax-exempt 501(c) (6) corporation
- Have a fully populated Board of Directors
- Refined our Goals, Strategic Plan and Bylaws
- Will be upgrading our website
- Information on Board, Officers, Organization, and Strategic Plan can be found at:

  [http://www.generatorforum.org/about_us](http://www.generatorforum.org/about_us)
NAGF: Accomplishments

- Focus Annual Meeting on information transfer and training
  - Modeling, Essential Reliability Services including governor response improvements, and workshops on RAI and CIP V5
- Provided feedback on Polar Vortex Report
- Presented part of MISO Governor Frequency Response Webinar
- NAGF is a member of the Resources Subcommittee of the Operating Committee
- NAGF is a member of the Risk-Based Registration Advisory Group (RBRAG) and Reliability Assurance Initiative Advisory Group (RAIAG)
- NAGF providing generator feedback to NPCC RSC
Agenda

- NAGF Overview
- Current GO / GOP Issues
- Info Sharing: Lessons Learned
Current GO/GOP Issues

Looking at NERC:

• CIP v5 implementation
• CIP v6
• RAI
• Risk BasedRegistrations
• And all the other wonderful things that NERC does…”
NERC Reliability Standards Development Plan 2015-2017

• 7 projects extended from 2014 into 2015
  • Project 2012-09 Implementation of IRO Review (on hold pending completion of the TOP/IRO Revisions)
  • Project 2008-02 Undervoltage Load Shedding
  • Project 2008-02.5 Underfrequency Load Shedding
  • Project 2009-03 Emergency Operations (IRO-001)
  • Project 2010-05.2 Phase 2 of Protection System Misoperations: SPS/RAS
  • Project 2010-14.2 Phase 2 of BAL-004, BAL-005 and BAL-006
  • Project 2014-0X PRC-001 (Separating PRC-001 from Project 2014-03 Revisions to TOP/IRO Standards and Project 2007-06 System Protection Coordination)

GO/GOP implications
NERC Reliability Standards Development Plan 2015-2017

- 4 new projects were added for 2015
  - Project 2015-01 TPL Directives
  - Project 2015-02 Periodic Review of EOP-004, EOP-005, EOP-006 and EOP-008
  - Project 2015-03 Periodic Review of System Operating Limit Standards (FAC-010, FAC-011, and FAC-014)
  - Project 2015-04 Alignment of Definitions in Glossary of Terms used in NERC Reliability Standards and NERC Rules of Procedure, Appendix 2

Several members of the NAGF raised a concern regarding communications by ISO-NE, NYISO and NPCC that appear to be in conflict with current NERC standards and previously communicated guidance for NERC CIP-002-5.1 Criterion 2.6. Essentially, *the BES cyber system becomes a Medium Impact if designated as critical to derivation of IROLs*

Some plants received notification that their AVR/PSS status is critical to IROLs

“If the critical component of the plant/station is not specified”, then the whole plant should be considered Medium Impact – NERC guidance conflicts with RE guidance

Real Time Operations defined: 15 minute impact

VAR-002-3 R3 & R4: “no need to notify the TOP is the AVR/PSS is down for less than 30 minutes, or for a change in reactive capability restored within 30 minutes”

**NAGF researched, wrote letters and interfaced with NERC, REs, ISOs and GO/GOPs. Issue still in progress...**
GO / GOP issues

- Essential Reliability Services
  - Ramping, Reserve and Frequency Support
  - Voltage Support

- Cold Weather Preparations / Mitigation

- EPA’s Clean Power Plan under Section 111(d)

- The continually changing landscape
  - Capacity retirements
  - Availability of natural gas
  - Increasing penetration of Variable Generation

- Staffing
  - Aging workforce
    - Organizational knowledge retention
Agenda

- NAGF Overview
- Current GO / GOP Issues
- Info Sharing: Lessons Learned
Lessons Learned: AVRs

- During a DCS upgrade, the screen that indicates the condition of the AVR was revised by the contractor.
- Current interpretation of VAR-002-3 is that the AVR must be in ONLY the voltage control mode, unless directed by TOP, etc…
- Which of the below shows that the AVR is controlling Voltage?
  - Manage by exception – what’s different?
  - DCS work and outages can “reset the mental map” for operators

- Plant Staff not questioning the “new look” resulted in a self report…
Lessons Learned: Metcalf

• PG&E Metcalf Substation Incident 4/16/2013
• Received significant media attention after former FERC chairman Jon Wellinghoff emphasized the issue on 2/5/2014. Initial media coverage (2013) mentioned vandalism, despite this being a very professional, military style operation.

Background:
• 0058: Communication vaults for two communications providers damaged prior to substation attack: AT&T and (9 minutes later) Level 3 Communications.
• 0137: gunfire commenced
• 0141: first 911 call gets through via cell phone from nearby power plant.
• 0137 to ~0150: Fence vibration alarm, cameras automatically slew to fence line, nothing seen. Fence alarms triggered three times - bullets hitting fence. One severed the vibration alarm wiring, disabling system
• 0156 Nine police units begin arriving
• Attackers never entered the substation
Lessons Learned: Metcalf
Lessons Learned: Metcalf

Mitigation plans considered and/or implemented:

• Armed guards during the clean-up and repair of the transformers

• Video and infrared surveillance cameras that were outward looking, not just the fenceline – the threat used to be thieves stealing spools of copper from within the property, and the substation was prepared to deal with that threat before the incident. Now the threat is much different, and requires a different set of countermeasures.

• Ballistic shields and other protective measures installed around critical substation equipment and the substation itself.

• Tall grass and bushes in the vicinity of the substation were completely removed (PG&E had previously allowed natural growth to minimize environmental impact). Trees were trimmed such that the lowest branches were many feet in the air.
Lessons Learned: Metcalf

• Communications manhole covers are welded in place within ~1 mile of the substation. A maintenance hassle for the workers having to service the vaults, but it was deemed necessary.

• The company’s operations center and security center are being co-located, to foster better communications and cooperation between the two groups. They were previously over 100 miles apart, and also about that same distance from the substation.

• Incident response and recovery plans were updated and improved.

• Staff training was conducted on the incident, the new defenses installed, and new policies and procedures were implemented.

Most of these measures are designed to mitigate a repeat of that last attack. What form will the next attack take? How are your facilities vulnerable?
Lessons Learned: Metcalf

• **27 AUG 2014** – a new incident at Metcalf

• Fences cut (multiple locations)

• Construction Equipment stolen – media report
  
  • Forklift & copper spool(s)?

YOU GET WHAT YOU INSPECT, NOT WHAT YOU EXPECT
Lessons Learned

• Don’t make it easy for the “bad guys”
Lessons Learned: Metcalf

Q & A
Thank you!

www.GeneratorForum.org
EMS Outages Analysis and Lessons Learned

Sam Chanoski, Director, Situation Awareness and Event Analysis
SPP RE Spring Workshop
March 11, 2015
• Introduction - Why This is Important
• Cause Analysis Trends
• Outage Attribute Trends and Analysis
• Lessons Learned
• Q & A
• Introduction - Why This is Important
• Cause Analysis Trends
• Outage Attribute Trends and Analysis
• Lessons Learned
• Q & A
The Character of Harms

"Pick important problems and fix them"
Dr. Malcolm Sparrow
John F. Kennedy School of Government

Severity

Frequency

Harms

Avoid

Learn and Reduce

Inverse Cost-Benefit

Significance Threshold
What we learn, find and fix here…

...improves resilience when we get to here.
Disaggregating the Harms

Production and Operations Management

Tailor-made interventions

Parse the Risk

General Theory

Internal

External

Malcolm K. Sparrow, John F. Kennedy School of Government, Harvard University
Category 2b - Complete loss of SCADA, control or monitoring functionality for 30 minutes or more

Category 1h - Loss of monitoring or control, at a control center, such that it significantly affects the entity’s ability to make operating decisions for 30 continuous minutes or more. Examples include, but are not limited to the following:

- Loss of operator ability to remotely monitor, control Bulk Electric System (BES) elements, or both
- Loss of communications from SCADA RTUs
- Unavailability of ICCP links reducing BES visibility
- Loss of the ability to remotely monitor and control generating units via AGC
- Unacceptable State Estimator or Contingency Analysis solutions
Performance, Regulation, and Excellence

- Normal Performance
- Practical Minimum Acceptable
- Regulatory Minimum Acceptable
- Excellence
- Forums, Trades
- EA, Info Sharing
- CMEP

Slope ≈ resiliency metric?
• Introduction - Why This is Important
• **Cause Analysis Trends**
• Outage Attribute Trends and Analysis
• Lessons Learned
• Q & A
Root Causes

- A3 - Individual Human Performance, 3%
- A4 - Management / Organization, 30%
- A2 - Equipment / Material, 24%
- A1 - Design / Engineering, 15%
- AZ - Information LTA, 23%
- A5 - Communication, 4%
- AX - Overall Configuration, 1%
Top Root Causes

Information to determine cause LTA (AZ)
Testing of Design/Installation LTA (A1B4C02)
Software Failure (A2B6C07)
Insufficient Job Scoping (A4B3C08)
Inadequate Risk Assessment of Change (A4B5C04)
Contributing Causes

- A1 - Design / Engineering, 16%
- A2 - Equipment / Material, 33%
- A3 - Individual Human Performance, 9%
- A4 - Management / Organization, 26%
- A5 - Communication, 8%
- A6 - Training, 1%
- A7 - Other, 3%
- AX - Overall Configuration, 4%
Top Contributing Causes

Software failure (A2B6C07)
Design output scope LTA (A1B2C01)
Inadequate vendor support of change (A4B5C03)
Undesired operation of coordinated systems (A2B7C04)
Defective or failed equipment (A2B6C01)
Testing of Design/Installation LTA (A1B4C02)
Communication path LTA (A2B7C01)
System interactions not considered or identified (A4B5C05)
Post maintenance/post-modification testing LTA (A2B3C03)
Inadequate Risk Assessment of Change (A4B5C04)
• Introduction - Why This is Important
• Cause Analysis Trends
• Outage Attribute Trends and Analysis
• Lessons Learned
• Q & A
Characteristics of Complete EMS Outages
(Oct 1, 2013 – Dec 31, 2014)

- Scheduled Maintenance Activity occurring:
  - Yes, 19
  - No, 8

- CIP related Activity:
  - Yes, 3
  - No, 24

- Weekday:
  - Yes, 22
  - No, 5

- **Scheduled Maintenance in progress**
- **Outage Unforeseen**

Mean Complete Outage Restoration Time = 64 Minutes
2b Outage Restoration Time vs. Category vs. Event count

- **EMS Hardware**: 140 events, mean restoration time 160 minutes, 2 events with 12 minutes.
- **EMS Software**: 6 events, mean restoration time 60 minutes.
- **Facilities**: 6 events, mean restoration time 60 minutes.
- **Network Infrastructure**: 6 events, mean restoration time 60 minutes.
- **Human Performance**: 1 event, mean restoration time 140 minutes.

Legend:
- Blue bar: Mean Outage Restoration Time
- Orange box: Count

- **Scheduled Maintenance Activity occurring**
  - No, 51
  - Yes, 24

- **CIP related Activity**
  - No, 72
  - Yes, 3

- **Weekday**
  - No, 25
  - Yes, 50
Partial Outage Time of the Day
(Oct 1, 2013 – Dec 31, 2014)

Number of Events

- Scheduled Maintenance in progress
- Outage Unforeseen

0:00 - 2:00
2:00 - 4:00
4:00 - 6:00
6:00 - 8:00
8:00 - 10:00
10:00 - 12:00
12:00 - 14:00
14:00 - 16:00
16:00 - 18:00
18:00 - 20:00
20:00 - 22:00
22:00 - 24:00
Analysis of Partial Restoration Times
(Oct 1, 2013 – Dec 31, 2014)

Mean Partial Outage Restoration Time = 71 Minutes
1h Outage Restoration Time vs. Category vs. Event count

- EMS Hardware
- EMS Software - Ex Vendor
- EMS Software - HP
- EMS Software - Network Model
- EMS Software - Vendor Bug
- Facilities
- Network Infrastructure

Restoration Time in Minutes

Mean Outage Restoration Time

Number of Events

Count

0 10 20 30
0 5 10 15 20 25 30

NERC
North American Electric Reliability Corporation

RELIABILITY | ACCOUNTABILITY
Trend of the outage restoration time

Mean Complete Outage Restoration Time

Mean Partial Outage Restoration Time
• Introduction - Why This is Important
• Cause Analysis Trends
• Outage Attribute Trends and Analysis
• Lessons Learned
• Q & A
• Energy Management Systems (EMS) are extremely reliable
• EMS outages increase the risk to the real-time reliability of the grid
• EMS outages have NOT had an adverse impact to reliability
• 113 complete outages (Category 2b) reported through December 31, 2014; 24 event analyses in progress
• 84 partial outages (Category 1h) reported through December 31, 2014; 57 event analyses in progress
• 109 entities reported either a 1h or a 2b or both
  ▪ 49 experiencing multiple outages
• Several noticeable themes...
Common Themes for Complete Outages

- Facilities maintenance affecting EMS
  - Planned UPS work led to multiple events
  - Planned telecommunication facilities work led to multiple events

- Software failures
  - Bugs in network infrastructure firmware
  - Latent bugs in network encryption software
  - Bug in vendor front end code
  - Incorrect scripts

- Configuration
  - Firewall
  - Improper VLANs
  - Switch
  - Memory allocation
  - File system mounts
Common Themes for Partial Outages

- **Software bugs**
  - Contingency Analysis code
  - ICCP code
  - AGC code
  - Initialization routines

- **Modeling of external network**
  - Inadequate modeling of external facilities before equivalence
  - Incorrect statuses
  - Incorrect tap positions

- **Individual Human Performance and Organizational Challenges**
  - Set tuning parameters
  - Turn on automatic SE/CA runs
  - Alarm for failed SE/CA runs
Common Themes for Partial Outages

- **External Vendor or Contractor**
  - Leased lines from ATT, Verizon etc.
  - SONET ring maintenance

- **Hardware failure**
  - NIC Cards
  - Inverters
  - Routers

- **Failover Testing**
  - Incorrect procedures
  - Missing files
  - Corrupted executables
• Communicating with neighboring operators and Reliability Coordinator
• Decision making processes to man substations during an outage
• Increased vigilance during outages, partial monitoring from neighbors and RC
• Improving causal analysis of events
• Improving Event Analysis report quality
• Voluntary reporting, helping everyone get better
Opportunities for Improvement

• Change management, particularly in the context of job scoping
• Use of EMS test systems (aka sandbox, QA, dev)
• Network infrastructure testing
• Routine failover testing
• Vendor relationship
• Communication – internal and external
• Task scoping and job aids
• **LL20141201** Control System Network Switch Failure
• **LL20140902** Loss of EMS Dispatch Workstation Functionality Due to NTP Time Synchronization Device Misconfiguration
• **LL20140901** Redundant Network Interface Cards on EMS
• **LL20140802** Loss of EMS Monitoring and Control Functionality for More Than 30 Minutes
• **LL20140604** Loss of SCADA Due to Memory Resources Being Fully Utilized
• **LL20131003** Failure of EMS While Performing Database Update
• **LL20131002** SCADA Failure Resulting in Reduced Monitoring Functionality
Related NERC Lessons Learned

- **LL20130802** Indistinguishable Screens During a Database Update Led to Loss of SCADA Monitoring and Control
- **LL20130801** Inappropriate System Privileges Caused Loss of SCADA Monitoring
- **LL20130204** Failure of EMS Due to Over-Utilization of Disk Storage
- **LL20130203** SCADA Failure Resulting in Loss of Monitoring Functionality
- **LL20130202** EMS Loss of Operators’ User Interface Application
- **LL20130201** EMS System Outage and Effects on System Operations
• Introduction - Why This is Important
• Cause Analysis Trends
• Outage Attribute Trends and Analysis
• Lessons Learned
• Q & A
Additional Information

- ERO Event Analysis Program
  (http://www.nerc.com/pa/rrm/ea/Pages/EA-Program.aspx)

- NERC Lessons Learned
  (http://www.nerc.com/pa/rrm/ea/Pages/Lessons-Learned.aspx)

- NERC EMS conference presentations
  (http://www.nerc.com/pa/rrm/Resources/Pages/Conferences-and-Workshops.aspx)
Questions and Comments

Sam Chanoski
Director, Situation Awareness & Events Analysis
Office (404) 446-9706
Cell (404) 904-2480
sam.chanoski@nerc.net
Reliability Assurance Initiative

Risk-Based Compliance Monitoring & Enforcement
Golden Spread Electric Cooperative (GSEC)

- GSEC is a tax-exempt, consumer-owned public utility, organized in 1984 to provide low cost, reliable electric service for its 16 rural distribution cooperative Members, with a peak demand of nearly 1,600 MW.
Mustang Station & Antelope Elk Energy Center
Reliability Assurance Initiative

• Risk-Based Compliance Monitoring
  – Risk-Based Oversight Framework
    • Risk Elements
    • Inherent Risk Assessment
    • Internal Controls Evaluation
    • CMEP Tools
    • Planning and Execution of Compliance Audits
Reliability Assurance Initiative

- Risk-Based Enforcement
  - FFT Evolution
  - Risk Posed by Noncompliance
  - Compliance
  - Self-Logging
Entity Compliance Staff – To Do List

• Read through and understand the changes
  – Auditor Handbook and Checklist
  – IRA (Inherent, Control, Detection, Residual)
  – ICE (Preventative, Detective, Corrective)

• Map the changes to what is already being done → ICE
GSEC ICE Map

GSEC Internal Compliance
• Internal Compliance Plan
• Methodologies, Procedures, Guidelines

GSEC Internal Compliance (RAI/RBCMEP)
• Internal Compliance Plan
  – With ICE identified
• Methodologies, Procedures, Guidelines
  – With ICE identified
What does ICE look like?

Internal compliance heating up? ICE it. 7 Fast Steps to ICEing an Internal Compliance Program

1. Review the Annual ERO CMEP Implementation Plan or your entity’s IRA Report from the RE specific to your entity.

2. The RE provided a list of Reliability Standards in the Annual ERO CMEP Implementation Plan – use them to evaluate.

3. Pull out your past audit reports.

4. Grab your trusty ICP or draft a better one that follows the FERC guidelines (LINK NEEDED)

5. List out information from neighboring systems or Operations Agreements.

6. Spend some money on a consultant or do an internal independent evaluation

7. Entity information on internal controls associated with RE IRA – specifically, what is preventative, what is detective, what is corrective?
5 Keys to PRE-vent a NERCatastrophe!

1. Support – a corporate training program
2. Make it a priority – disable their computer until they complete training
3. Start something new – reliability department, anyone?
4. Keep track - Management approval of deviation from standard maintenance cycle
5. Cut out the humans - any outage on the system is automatically recorded and sent to management for review.
3 Steps to Detect a NERC Meltdown

1. Talk – Check-in Schedule
   1. A schedule announced in advance that indicates when you will check with staff for compliance priorities.

2. Test – Standardize evidence gathering that indicates when evidence is needed and exactly what is needed.

3. Follow-up – Consistently do any action steps or confirm action steps are done to maintain compliance.
Risk-Based Compliance Monitoring

John Allen – Manager Reliability Compliance
City Utilities of Springfield

- **Service Area**
  - Population: 229,000
  - Size (in square miles): 320

- **Electric System**
  - Customers (Avg.): 110,587
  - Hourly Peak Demand: 802 MW (8/3/2011)

- **Natural Gas**
  - Customers (Avg.): 82,739
  - Daily Peak Demand: 131,487 Dth (1/12/2011)

- **Water**
  - Customers (Avg.): 80,681
  - Daily Peak Demand: 59.4 MG (8/13/2007)

- **Transit**
  - Miles of Route: 185

- **SpringNet Telecommunications**
  - Customers: 818
  - Miles of Fiber: 429
City Utilities of Springfield

• 120 Miles Transmission >100 kV
• 92 Miles Transmission @ 69 kV
• 43 Substations
• Interconnections @ 6 Substations
• 1034 MW (Net) Generation
• 802 MW Summer Peak (August 2011)
NERC Registrations

1. Transmission Owner
2. Transmission Operator
3. Generator Owner
4. Generator Operator
5. Distribution Provider
6. Load Serving Entity
7. Transmission Planner
8. Resource Planner
Governance Structure

- 11 Member Board of Public Utilities
- City Council
  - Appoints Board Members
  - Approves Budget
- General Manager
Compliance Program

• Senior Manager (CIP & Ops/Planning)
  o Reviews and approves CIP Policy
  o Ensures funding of compliance activities
  o Informs General Manager as needed
Compliance Program

- Executive Involvement
- Compliance Officer
  - Approves all compliance programs
  - Independent access to General Manager
Compliance Program

• Manager Reliability Compliance
  o Administers all compliance programs

• Reliability Compliance Specialist
  o Ops/Planning

• CIP Compliance Specialist
  o Critical Infrastructure Protection
Compliance Committee

- Board of Public Utilities
  - General Manager
    - Associate General Manager - Operations
      - Director - Distribution
      - Manager - Physical Security
      - Assistant Manager - Transmission and Distribution
    - Associate General Manager - IT and Transportation
      - Manager - IT Infrastructure
    - Associate General Manager - Electric Supply
      - Director - Electric Supply
      - Manager - Power Generation
      - Manager - Reliability Compliance
    - Associate General Manager - General Counsel
      - Director - Power System Control
      - Director - Transmission Planning and Compliance

* Compliance Committee Members
Compliance Goals

• Monitor NERC/SPP Activities
• Best Practices
• Maintain Audit Ready Status
• NERC Training for SMEs
• Zero Violations
Internal Risk Assessment

• Probability of Violation
• Consequences of Violation
Probability of Violation

- Age
- Audit History
- Ownership
- SME Performance
- Event Driven
Consequences of Violation

- Violation Risk Factor
- AML List
- Top 10 Violated
- Violation History
Internal Controls

- Policies, Plans, Programs, Procedures, etc.
- Document Management (SharePoint)
- Workflow Tools (Cascade, BPLogix)
- Quarterly Surveys
- Self-Assessments
### SharePoint Site

#### Electric Reliability Compliance > Standards and Compliance

**Advanced Search**

<table>
<thead>
<tr>
<th>Type</th>
<th>Name</th>
<th>Modified</th>
<th>Modified By</th>
<th>Next Review Date</th>
<th>Version</th>
</tr>
</thead>
<tbody>
<tr>
<td>Agreement-Contract</td>
<td></td>
<td>2/10/2012 2:02 PM</td>
<td>System Account</td>
<td></td>
<td>1.0</td>
</tr>
<tr>
<td>Analysis</td>
<td></td>
<td>2/13/2012 9:40 AM</td>
<td>System Account</td>
<td></td>
<td>1.0</td>
</tr>
<tr>
<td>Attestation</td>
<td></td>
<td>2/10/2012 3:11 PM</td>
<td>System Account</td>
<td></td>
<td>1.0</td>
</tr>
<tr>
<td>Drawing</td>
<td></td>
<td>2/10/2012 3:20 PM</td>
<td>System Account</td>
<td></td>
<td>1.0</td>
</tr>
<tr>
<td>Email</td>
<td></td>
<td>2/10/2012 3:20 PM</td>
<td>System Account</td>
<td></td>
<td>1.0</td>
</tr>
<tr>
<td>HR-Training Records</td>
<td></td>
<td>2/10/2012 3:31 PM</td>
<td>System Account</td>
<td></td>
<td>1.0</td>
</tr>
<tr>
<td>Industry Standards-Guidelines</td>
<td></td>
<td>2/10/2012 3:31 PM</td>
<td>System Account</td>
<td></td>
<td>1.0</td>
</tr>
<tr>
<td>Job Description</td>
<td></td>
<td>2/10/2012 3:42 PM</td>
<td>System Account</td>
<td></td>
<td>1.0</td>
</tr>
<tr>
<td>Letter</td>
<td></td>
<td>2/10/2012 3:42 PM</td>
<td>System Account</td>
<td></td>
<td>1.0</td>
</tr>
<tr>
<td>Maintenance Record</td>
<td></td>
<td>10/11/2013 1:43 PM</td>
<td>System Account</td>
<td></td>
<td>1.0</td>
</tr>
<tr>
<td>Map</td>
<td></td>
<td>3/11/2014 9:53 AM</td>
<td>System Account</td>
<td></td>
<td>1.0</td>
</tr>
<tr>
<td>Meeting Agenda-Minutes</td>
<td></td>
<td>2/10/2012 4:01 PM</td>
<td>System Account</td>
<td></td>
<td>1.0</td>
</tr>
<tr>
<td>Not Sure</td>
<td></td>
<td>10/27/2011 12:57 PM</td>
<td>System Account</td>
<td></td>
<td>1.0</td>
</tr>
<tr>
<td>Policy-Procedure</td>
<td></td>
<td>2/10/2012 4:01 PM</td>
<td>System Account</td>
<td></td>
<td>1.0</td>
</tr>
<tr>
<td>Presentation-Training Lesson</td>
<td></td>
<td>2/10/2012 4:36 PM</td>
<td>System Account</td>
<td></td>
<td>1.0</td>
</tr>
<tr>
<td>Report</td>
<td></td>
<td>2/10/2012 4:34 PM</td>
<td>System Account</td>
<td></td>
<td>1.0</td>
</tr>
<tr>
<td>RSAW</td>
<td></td>
<td>2/11/2012 6:15 PM</td>
<td>System Account</td>
<td></td>
<td>1.0</td>
</tr>
<tr>
<td>Screenshot</td>
<td></td>
<td>2/11/2012 6:35 PM</td>
<td>System Account</td>
<td></td>
<td>1.0</td>
</tr>
<tr>
<td>Voice Recording</td>
<td></td>
<td>2/11/2012 6:50 PM</td>
<td>System Account</td>
<td></td>
<td>1.0</td>
</tr>
</tbody>
</table>

*Add document*
<table>
<thead>
<tr>
<th>Standard</th>
<th>Requirement</th>
<th>Title</th>
<th>Current Date</th>
<th>Due Date</th>
<th>Document #</th>
</tr>
</thead>
<tbody>
<tr>
<td>TOP-001</td>
<td>1</td>
<td>Reliability Coordination-Responsibilities and Authority policy</td>
<td>11/12/2014</td>
<td>11/12/2015</td>
<td>Policy 0031</td>
</tr>
<tr>
<td>FAC-001</td>
<td>1</td>
<td>CU Facility Connection Requirements</td>
<td>11/13/2014</td>
<td>11/13/2015</td>
<td>Policy 0051</td>
</tr>
<tr>
<td>IRO-001</td>
<td>8</td>
<td>Reliability Coordination-Responsibilities and Authorities policy</td>
<td>11/13/2014</td>
<td>11/13/2015</td>
<td>Policy 0024</td>
</tr>
<tr>
<td>IRO-005</td>
<td>10</td>
<td>Reliability Coordination — Current Day Operations policy</td>
<td>11/13/2014</td>
<td>11/13/2015</td>
<td>Policy 0027</td>
</tr>
<tr>
<td>COM-001</td>
<td>2</td>
<td>Telecom Master Maintenance Plan</td>
<td>11/19/2014</td>
<td>11/19/2015</td>
<td>Process 0048</td>
</tr>
<tr>
<td>PER-005</td>
<td>1</td>
<td>Substation Training Policy</td>
<td>12/1/2014</td>
<td>12/1/2015</td>
<td>Policy 0001</td>
</tr>
<tr>
<td>PRC-001</td>
<td>2</td>
<td>Transmission Relay Equipment Failures</td>
<td>12/1/2014</td>
<td>12/1/2015</td>
<td>Policy 0002</td>
</tr>
<tr>
<td>PRC-001</td>
<td>3</td>
<td>Transmission Protection System Coordination</td>
<td>12/1/2014</td>
<td>12/1/2015</td>
<td>Policy 0003</td>
</tr>
<tr>
<td>PRC-004</td>
<td>1</td>
<td>Transmission Protection System Operations Analysis</td>
<td>12/1/2014</td>
<td>12/1/2015</td>
<td>Process 0002</td>
</tr>
<tr>
<td>PRC-005</td>
<td>1</td>
<td>Substation Inspection Policy</td>
<td>12/1/2014</td>
<td>12/1/2015</td>
<td>Policy 0004</td>
</tr>
<tr>
<td>PRC-010</td>
<td>1</td>
<td>UVLS Statement</td>
<td>12/1/2014</td>
<td>12/1/2015</td>
<td>Policy 0005</td>
</tr>
<tr>
<td>PRC-015</td>
<td>1</td>
<td>SPS Statement</td>
<td>12/1/2014</td>
<td>12/1/2015</td>
<td>Policy 0006</td>
</tr>
<tr>
<td>PRC-018</td>
<td>1</td>
<td>DME Statement</td>
<td>12/1/2014</td>
<td>12/1/2015</td>
<td>Policy 0007</td>
</tr>
<tr>
<td>PRC-023</td>
<td>1</td>
<td>Transmission Relay Loadability Statement</td>
<td>12/1/2014</td>
<td>12/1/2015</td>
<td>Policy 0048</td>
</tr>
<tr>
<td>PER-005</td>
<td>1</td>
<td>Operating Personnel Training policy</td>
<td>12/1/2014</td>
<td>12/1/2015</td>
<td>Policy 0028</td>
</tr>
<tr>
<td>PRC-001</td>
<td>1</td>
<td>Power System Control Protection Systems policy</td>
<td>12/1/2014</td>
<td>12/1/2015</td>
<td>Policy 0030</td>
</tr>
</tbody>
</table>
### Workflow Tool (BPLogix)

<table>
<thead>
<tr>
<th>Change Request Information</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Date Submitted:</strong> 1/26/2015</td>
</tr>
<tr>
<td><strong>Request Number:</strong> 201501262925</td>
</tr>
<tr>
<td><strong>Requestor Name:</strong> Bob Ruzicka</td>
</tr>
<tr>
<td><strong>Patch Tracking Number:</strong></td>
</tr>
<tr>
<td><strong>Product:</strong></td>
</tr>
<tr>
<td><strong>Request Type:</strong></td>
</tr>
<tr>
<td><strong>Category:</strong> Software</td>
</tr>
<tr>
<td><strong>Is testing required?</strong></td>
</tr>
</tbody>
</table>

**Assets:**
Workflow Tool (Cascade)
Workflow Tool (Cascade)
Quarterly Surveys

Transmission and Distribution
NERC Compliance Survey
4th Quarter 2014
Due: January 16, 2015

1. During this quarter did you add any new facilities to the transmission system? [ ]
   If yes, did this new facility change the ratings of any other existing facilities? [ ]
   Explain: [ ]

   (Submit updated documentation.)
   [ ]

2. During this quarter did you add, remove or replace any element or modify any relay settings on a transmission facility? [ ]
   If yes, did you update the Facility Rating Sheet? [ ]

   (Submit updated documentation.)
   [ ]

3. During this quarter did you coordinate all protection system changes made to interconnecting systems with the neighboring utility(ies)? [ ]

   (Submit updated documentation.)
   [ ]
RBCM Activities

- Inherent Risk Assessment
- Internal Control Evaluation
- BES Exceptions
- Risk Based Registration
- Self-Logging Violations
Questions?
Internal Risk-based Compliance Monitoring
March 11, 2015
Risk-based Compliance Monitoring

- Governance Framework
- Risk Assessment
- Internal Compliance Assessment
- Internal Audit Role
- Moving Forward
Governance Framework

- Regulatory Compliance Program
- Executive Steering Committee
- Non-compliance reporting & mitigation
- Communication and Training
Risk Assessment

- Categorize as High, Medium, Low risk
- Likelihood, Impact, Company Risk Evaluation
- Each year the approach is refined
Internal Compliance Assessment

- Completed annually
- Utilize Risk Assessment results
- Documents management practices and controls
- Assesses compliance evidence and structure
- Identifies enhancements, concerns, non-compliance
- Utilized as ‘mock audit’ opportunity as appropriate
- Internal Audit and Legal participation
- Summary results documented in Evidence Roadmap
## Evidence Roadmap Example

<table>
<thead>
<tr>
<th>Requirement</th>
<th>Requirement Description</th>
<th>RSAW Compliance Assessment Approach</th>
<th>RSAW Narrative Response</th>
<th>Evidence Reviewed</th>
</tr>
</thead>
<tbody>
<tr>
<td>R1</td>
<td>Each Reliability Coordinator, Balancing Authority, and Transmission Operator shall have a current Operating Plan describing the manner in which it continues to meet its functional obligations with regard to the reliable operations of the BES in the event that its primary control center functionality is lost. This Operating Plan for backup functionality shall include the following, at a minimum:</td>
<td>Reference WR EOP-008-1 RSAW 2014.docx located in the NERC Compliance SharePoint site under Compliance RSAWs library.</td>
<td>Westar Energy (Westar) has a current Operating Plan (SO 750-01 Operating Plan for Loss of Primary Control Center Functionality) that describes the manner in which it continues to meet its functional obligations with regard to the reliable operations of the BES in the event that its primary control center functionality is lost. The Plan includes an Operating Process for keeping the backup functionality consistent with the primary control center functionality.</td>
<td>1) SO 750-01 Operating Plan for Loss of PCC Functionality 20140601 2) bucc gso Checklist 20140603 001.pdf</td>
</tr>
</tbody>
</table>

### Evidence Location

- R:\NERC Reliability\2014 Compliance Evidence

### Evidence Owner(s)

- Bryan Taggart and Allen Klassen

### Evidence Review Notes

- Reviewed the SO 750-01 Operating Plan for Loss of PCC Functionality 20140601 to verify that all elements listed in R1 are covered in the plan. Also reviewed the GSO-BUCC Systems Consistency Checklist to verify a periodic check was done on 6/3/14.

### Conclusion

- Compliant

### Enhancement/Concern

- Annual review of Operating Plan for Loss of Primary Control Center Functionality.

### Internal Controls

- System Operators conduct periodic drills of the Operating Plan for Loss of PCC Functionality. As part of the drill, a checklist is completed.

### Internal Control Type

- Preventative

- Detective
Internal Audit Department Role

- Independent risk assessment of the Program
- Periodic evaluation of compliance with the Program
- Participation in higher risk Compliance Assessment areas
- Independent evaluation of specific Standards as appropriate
Moving Forward

• Continue to align our internal efforts with NERC approach
• Formally presented to our Executive Staff in January 2015
• Focus resources on higher risk areas
• Improve documentation of management practices and controls
• Positive impact on reliability
Questions

Bo.Jones@westarenergy.com

785.575.1680
• Far-end Relay
• Programmable Devices
• Generation Segmentation
• Virtualization (Networks and Servers)
• Serial Devices that are accessed remotely
• Control Centers operated by TOs and non-registered BAs
• Interactive Remote Access (Scripts and Mgt consoles)
• 3rd Party Notifications of medium impact assets
• Mixed Trust EACMs
• Network devices as BES Cyber Systems
• General FAQs
Far-end Relay (AKA Transfer-Trip)
- Approved by the Standards Committee to be published as a Lesson Learned.
- **Final** position: the far-end relay does not automatically inherit a Medium impact categorization if the near-end substation satisfies the qualifications of Criterion 2.5.
Programmable Electronic Devices (Draft)

• **Programmable Electronic Device (PED)** – A Programmable Electronic Device (PED) has a microprocessor and field-updateable firmware, software or logic.
  - Field-Updatable” would include devices that have a management port, web interface, or any external interface that would allow the introduction of a firmware, software or logic update by a customer or field-service technician.

• **Configurable-only Device (Non-PED)** - A device that will not allow user changes to its internal programming, but otherwise allows the user to change between pre-defined operational parameters or change hardware options, is configurable.
  - If a parameter allows for the entry of formulas, functions and/or any other series of logic steps then this would constitute “Programming” and would make the device a PED.
  - Posted for comment in January
  - Should be final by April 1, 2015
• Generation Segmentation
  – Approved by the Standards Committee to be published as a Lesson Learned.
  – Final Position: BES Cyber Systems associated with a generating plant in excess of 1500 MW Net Real Power Capability can be segmented such that there are no Medium impacting BES Cyber Systems.
  – Includes a discussion of evidence required to demonstrate sufficient segregation.
Virtualization (Networks and Servers)

- Will be published as two Lessons Learned by April 1, 2015
  
  - Virtual Machines (VM)
  
  - Virtual Local Area Networks (VLAN)

- Current position:
  
  - The Virtual Host and hypervisor inherits the categorization of the highest impact Guest OS
  
  - CIP-005-5, Requirement R1, Element 1.1 requires entire Virtual Environment or virtualized communication/network device to reside fully within or outside of the Electronic Security Perimeter. Mixed mode/mixed trust environments are being evaluated for compliance considerations.
• Serial Devices that are accessed remotely
  – V5TAG is evaluating a SAR and interim guidance
  – Two competing positions:
    ▪ Serially connected devices do not have to reside with an Electronic Security Perimeter, therefore are excluded from Cyber Assets with External Routable Connectivity even if connected to a terminal server that does communicate with a routable protocol.
    ▪ The terminal server converting from routable to serial protocol does not exclude serially connected Cyber Assets if the communication is essentially a pass-through and the remote user or Cyber Asset is accessing and manipulating the serially connected local Cyber Asset.
Control Centers operated by TOs and non-registered BAs

- Expected to be posted for comment by 2/27/15.
- Concern is with Control Centers of entities not registered as TOPs but actually controlling the generation or substation assets from the local SCADA/EMS under instruction from the registered BA or TOP.

High Impact Rating (H)

- 1.2. Each Control Center or backup Control Center used to perform the functional obligations of the Balancing Authority: 1) for generation equal to or greater than an aggregate of 3000 MW in a single Interconnection, or 2) for one or more of the assets that meet criterion 2.3, 2.6, or 2.9.
- 1.3 Each Control Center or backup Control Center used to perform the functional obligations of the Transmission Operator for one or more of the assets that meet criterion 2.2, 2.4, 2.5, 2.7, 2.8, 2.9, or 2.10.

Medium Impact Rating (M)

- 2.12. Each Control Center or backup Control Center used to perform the functional obligations of the Transmission Operator not included in High Impact Rating (H), above.
- 2.13. Each Control Center or backup Control Center, not already included in High Impact Rating (H) above, used to perform the functional obligations of the Balancing Authority for generation equal to or greater than an aggregate of 1500 MW in a single Interconnection.
Interactive Remote Access (Scripts and Management Consoles)

- The question is whether scripts under programmatic control and actions performed by management consoles constitute Interactive Remote Access.
  - Can perform the exact same process interactively.
  - Cannot distinguish between true interactive access and programmatic access from a system or network perspective.

- Initial position is that such access is Interactive Remote Access.

- Comment period closed in February 2015.
• Generation Interconnection (definition)
  – Expected to be posted for comment by 2/27/15.
  – Current position
    ▪ The question is whether the line (sometimes referred to as the generator lead line) operated at transmission voltages between a generating plant and a transmission substation is a Transmission Facility for the purposes of the CIP-002-5 Impact Rating Criteria.
    ▪ Current position: For a Transmission line to be considered a Transmission Facility and included in the Criterion 2.5 calculation, the line must be used for network flow of the Bulk Electric System and connected to another Transmission station or substation.
• Mixed Trust Electronic Access Control or Monitoring Systems
  – The issue is whether corporate resources (Active Directory servers, remote access authentication servers, log servers, Intrusion Detection Systems, etc.) supporting both corporate and Electronic Security Perimeter access control are Electronic Access Control or Monitoring Systems.
  – Initial position is that if the Cyber Asset is providing electronic access control or monitoring support to the CIP environment, the Cyber Asset is an EACMS for the purposes of CIP compliance.
  – Comment period closed in February 2015
Network Devices and BES Cyber Systems

- Exclusion: Cyber Assets associated with communication networks and data communication links between discrete Electronic Security Perimeters.

- Some entities have read the above to mean that all communications networks are excluded for the scope of CIP.

- Data communication links between ESPs are excluded.

- How should communication links between BCS be considered if ESPs are not identified?

- Current thought: Define an in-scope/out-of-scope demarcation point in the absence of a defined ESP.

- Will be posted for comment by April 1, 2015
What’s Trending with CIP V5 Transition

- General Frequently Asked Questions (FAQs)
  - 3 are already posted on the V5 Transition Program page on the NERC web site as “Technical FAQs”
  - Will be updated on a regular basis as questions are received and answers formulated.
  - Estimated to address 50-80 additional areas of content.
CIP-10-2 Change Management

March 10, 2015

Steven Keller
Lead Compliance Specialist - CIP
skeller.re@spp.org · 501.688.1633
CIP-10-2 BASICS R1 AND R2
What is CIP-010-2?

• The configuration change management processes are intended to prevent unauthorized modifications to BES Cyber Systems
• Understand what is on your system(s)
• Be aware of authorized or unauthorized changes to any and all BES Cyber Systems
• Baselines, Baselines, Baselines
V5 vs V3 for CIP-10-2 R1 and R2

• CIP-003-3 R6: Change Control and Configuration Management

• CIP-007-3 R1: Testing

• Requirement applies to all BES Cyber Assets within the identified BES Cyber System(s)
CIP-010-2 R1.1 Requirement

• Develop a baseline configuration, individually or by group, which shall include the following items:

1.1.1. Operating System or firmware where no independent OS exits

1.1.2. Any commercially available or open source application software intentionally installed

1.1.3. Any custom software installed

1.1.4. Any logical network accessible ports

1.1.5. Any security patches applied
CIP-010-2 R1.1 Baseline Minimum

- Five Basic required items to include in your baseline:
  1. OS Software or firmware
  2. Intentionally installed commercial and/or open source software
  3. Any custom applications
  4. Open logical network accessible ports
  5. Security patches that have been applied
CIP-010-2 R1.2 Requirement

• Authorize and document changes that deviate from the existing baseline configuration
CIP-010-2 R1.2 Approach

- Who is authorized to approve changes?
- Who is allowed to make those changes?
- How will you document those changes?

- Do not allow the approver of the changes to be the one making the changes
CIP-010-2 R1.3 Requirement

• For a change that deviates from the existing baseline configuration, update the baseline configuration as necessary within 30 calendar days of completing the change.
CIP-010-2 R1.3 Approach

- Baseline should be updated 30 days after that patch was installed or software updated
For changes that deviate from existing baseline configuration:

1.4.1. Prior to the change, determine required cyber security controls in CIP-005 and CIP-007 that could be impacted by the change;

1.4.2. Following the change, verify that required cyber security controls determined in 1.4.1 are not adversely affected; and

1.4.3 Document the results of the verification.
CIP-010-2 R1.4 Approach

• What are those controls?
• Controls for Windows vs. Unix vs. Cisco
• Verify all changes made to baseline are properly documented and approved
• What evidence do you have to show controls were tested and not adversely affected?
CIP-010-2 R1.5 Requirement

• Where technically feasible for each change that deviates from the existing baseline configuration:

1.5.1. Prior to implementing any change in the production environment, test the changes in a test environment or test the changes in a production environment where the test performed in a manner that minimizes adverse effects, that models the baseline configuration to ensure that required cyber security controls in CIP-005 and CIP-007 are not adversely affected; and
CIP-010-2 R1.5 Req. – Cont.

• Where technically feasible for each change that deviates from the existing baseline configuration:

  1.5.2. Document the results of the testing and, if a test environment was used, the difference between the test environment and the production environment, including a description of the measures used to account for any difference in operation between the test and production environment.
CIP-010-2 R1.5 Approach

• Applies to High Impact BES Cyber Systems
• If a test environment was used, must document the difference between test and production environments
• List those controls tested and document the results of those tests
CIP-010-2 R2.1 Requirement

- Monitor at least once every 35 calendar days for changes to the baseline configuration (as described in Requirement R1, Part 1.1).
- Document and investigate detected unauthorized changes
CIP-010-2 R2.1 Approach

- Monitor for changes at least once every 35 days
- What is the monitoring process? How do you ensure you do not miss the 35 day deadline?
- Logs, change tickets, or tracking sheets?
- Keep your records and know where they are kept
- Is there a file monitoring tool that can be used?
Total SPP Events for 2014

- 30 total events, 13 Category 1 Events, 3 Category 2 events analyzed via NERC’s Event Analysis process
SPP Regional Events (October 1\textsuperscript{st} – December 31\textsuperscript{st})

- One category 1h. Partial loss of monitoring or control, at a control center for 30 min
- One category 1a. An unexpected outage, contrary to design, of three or more BPS facilities
- One category 2a. Complete loss of SCADA, control or monitoring for 30 min
Loss of SCADA

- Technician Error
- Technician accidently cut fiber optic cable
- SCADA communication was lost to
  - Fifteen 69KV substations
  - Four 161 KV substations
  - Two generating stations
- Event lasted 133 minutes
Three Phase Fault

• 345 KV Phase fell onto 230 KV line
• Top portion of structure on fire and broken free
• 345 KV line was in contact with all three phases of the 230 KV line
• Equipment lost
  – 345 KV line
  – Two 230 KV lines
  – One 115 KV line
  – One Unit 750 MW generation online at time of trip
Complete loss of SCADA

- Failed failover test resulted in complete loss of EMS
- Failover test from the Backup site
- EMS staff on site at Primary unable to bring primary and back-up systems back online
- Primary was rebooted
- Duration 43 minutes
NERC LESSONS LEARNED
Control System Network Switch Failure

- Partial failure of a core switch for two units but allowed ports to stay open
- Secondary switch detected failure opened its ports for communication
- Simultaneous operation caused network to loop generating a data storm
- Data storm blocked communication to unit controls
Control System Network Switch Failure

- Lesson Learned
  - Redundant devices may introduce unanticipated scenarios if not fully tested
  - Consider external monitor for diagnostics and alarming
  - Testing of network topology and failover
Bus Differential Power Supply Failure

- The differential relay power supply capacitor started degrading
- The failing capacitor caused the analog to digital converter to give erroneous current and voltage values
- This resulted in an “A” phase bus trip on bus 1 and bus 2
- 58,000 customers lost
Bus Differential Power Supply Failure

• Corrective Actions

– The affected DC power supplies were replaced with new versions of power supplies that incorporate additional self-monitoring
Bus Differential Power Supply Failure

- **Lesson Learned**
  - For high impact schemes, supervision should be independent of the tripping device.
  - If one scheme is used to trip two busses, then there should be increased security when applied.
  - Relay manufacturers should ensure there is sufficient device monitoring.
Loss of Generators Due to Control Air

• Multiple issues with Generators tripping due to control air

• **Corrective Actions**
  – Procedural changes to reduce non-critical air usage
  – Reconfigure electrical supply to air compressors so that the loss of one source would not trip multiple air compressors
  – Install additional air compressors
Loss of Generators Due to Control Air

• Lesson Learned
  – Plant personnel should be aware that when headers are tied together, a problem could result in multiple units tripping.
FAC Alert January 15th 2015

• Remediation

100% of the High priority lines are complete

72% of the Medium priority lines are complete

75% of the Low priority lines are complete
Links

• SPP RE Event Analysis Webpage
  http://www.spp.org/section.asp?pageID=142

• Event Analysis Process Documents

• SPP Lessons Learned

• NERC Lessons Learned
### Internal Control Tab

**Internal Control Evaluation Workbook**

<table>
<thead>
<tr>
<th>Entity Name:</th>
<th>Acme Power &amp; Light</th>
</tr>
</thead>
<tbody>
<tr>
<td>NCR:</td>
<td>NCRXXXXXX</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Standard</th>
<th>Requirement</th>
<th>ICE Optional</th>
<th>Entity Desires Review</th>
<th>Date Control Implemented</th>
<th>Entity has had External/Internal Audit of control</th>
<th>SPP RE will review design</th>
<th>SPP RE will test effectiveness</th>
</tr>
</thead>
<tbody>
<tr>
<td>SPPRE</td>
<td>SPPRE</td>
<td>SPPRE</td>
<td>Entity(Y/N)</td>
<td>Entity(Date)</td>
<td>Entity(Y/N)</td>
<td>SPPRE</td>
<td>SPPRE</td>
</tr>
</tbody>
</table>

### Identifying Key Controls Tab

**Internal Control Evaluation Workbook**

<table>
<thead>
<tr>
<th>Entity Name:</th>
<th>Acme Power &amp; Light</th>
</tr>
</thead>
<tbody>
<tr>
<td>NCR:</td>
<td>NCRXXXXXX</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Risk Factor</th>
<th>Entity Provided Internal Control</th>
<th>Key Control</th>
<th>Rationale</th>
</tr>
</thead>
<tbody>
<tr>
<td>Description of Risk concept (stds and reqts)</td>
<td>Description of internal control (1-3 sentences)</td>
<td>Yes/No</td>
<td>1-3 sentences.</td>
</tr>
</tbody>
</table>
### Internal Control Design Tab

<table>
<thead>
<tr>
<th>Risk factor</th>
<th>Key Internal Control</th>
<th>Assess Information</th>
<th>Evidence to Support Conclusion</th>
<th>Standard well designed?</th>
</tr>
</thead>
<tbody>
<tr>
<td>Risk concept (stds and reqts)</td>
<td>Description of internal control (1-3 sentences)</td>
<td>Credibility:</td>
<td>2-3 examples (bulleted)</td>
<td>Yes/No</td>
</tr>
<tr>
<td>Sufficiency:</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

### Internal Control Test Plan Tab

| Entity Name: | Acme Power & Light |
| NCR: | NCRXXXXXX |

<table>
<thead>
<tr>
<th>Std/Req.</th>
<th>Key Internal Control</th>
<th>Documentation of Implementation requested</th>
</tr>
</thead>
<tbody>
<tr>
<td>FAC-008-3 R6.</td>
<td>Construction Review (list)</td>
<td>List desired documentation or say provided sampled data from “sample file”, etc.</td>
</tr>
<tr>
<td>Standard</td>
<td>Key Preventative Controls</td>
<td>Effectiveness of Implementation</td>
</tr>
<tr>
<td>-----------</td>
<td>--------------------------</td>
<td>--------------------------------</td>
</tr>
<tr>
<td>FAC-008</td>
<td>(description #1)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>(description #2)</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

ICE Evaluation
Objectives

• Describe the SPP RE IRA process
• Describe the SPP RE ICE process
• Describe the tools used for IRA and ICE
• Explain the use of the IRA and ICE results
Inherent Risk Assessment (IRA) Process

- Why is SPP RE doing an Inherent Risk Assessment?
  - To develop the Registered Entity’s compliance oversight plan
    - Identify the level of risk to the BPS
    - Monitoring scope
    - Monitoring method
    - Monitoring frequency
  - To understand the Registered Entity so we can assess the risks
Process Steps

Information Gathering
- Gather Risk Elements Module Output
  - Determine Entity Specific Information Needs to Perform IRA
  - Develop Targeted Information Request List

Assessment
- Risk Factor and Standards and Requirements Applicability Review
  - Risk Factor Analysis
  - Review of IRA Conclusions

Results
- Results Documentation
  - Draft Compliance Oversight Plan for Registered Entity
Information Gathering

• SPP RE’s IRA Questionnaire
• SPP RE’s Asset Spreadsheet
• Internal information
  – Previous audit reports
  – Self-certifications
  – Reliability Coordinator Questionnaire
  – Compliance history
Assessment

- **SPP RE’s IRA Template**
  - Compliance history – Open Enforcement Actions and mitigations
  - Technical assessment risk factor criteria were developed using the Appendix C of the *ERO Enterprise Inherent Risk Assessment Guide*.

<table>
<thead>
<tr>
<th>Risk Factor</th>
<th>Criteria</th>
</tr>
</thead>
<tbody>
<tr>
<td>Registration</td>
<td>Function: PSE, LSE, DP, GO, GOP, TO, IA, PA, RC, BA, TOP</td>
</tr>
<tr>
<td>Geography/Climate</td>
<td>Flat or no identified issues, Moderate terrain issues (list), Mostly rugged terrain, mountains, oceans</td>
</tr>
<tr>
<td>Vegetation Management</td>
<td>Little or no trees (plains; desert), Moderate climate, Invasive climate or past identified issues</td>
</tr>
</tbody>
</table>
Assessment

• CIP information – SCADA/EMS information, Firewalls, Network vendors, workstations ...

• Internal Control Evaluation (ICE) assessment – if the Registered Entity requested an evaluation of internal controls

• Joint Registration Organization/Coordinated Functional Registration

• Monitoring scope is determined by using the ERO and SPP RE Risk Elements and the Registered Entity’s attributes

• Entity’s Qualitative assessment
  • Identifies the Entity’s Transmission Operator, Balancing Authority, Reliability Coordinator and Planning Authority
  • Summary of the technical assessments
Results

• The IRA will be presented by the lead auditor to the SPP RE IRA Review Team for evaluation of the results
• Upon completion of the review, the auditor will present to SPP RE management for approval
• The results will describe:
  • Identify the risk areas
  • Scope of the engagement
  • Oversight plan
• The Registered Entity will be presented with an assessment letter with the results to allow for clarity and transparency in the assessment process
Summary of the Assessment

• The IRA Assessment Letter will be sent to the Registered Entity at the conclusion of the Inherent Risk Assessment

• SPP RE will ask the Registered Entity if they would like an Internal Control Evaluation (ICE) performed for any of the requirements in their audit scope

• At this point, the ICE process will begin
Internal Control Evaluation Process

• How does a Registered Entity request an ICE?

• With the IRA Assessment Letter you will receive an Internal Control Evaluation Workbook

• What is in the Workbook?
  – List of the Standards/Requirements that are in scope
  – The Registered Entity will identify the Standard/Requirement for which they want an ICE performed
  – SPP RE will review the list of controls the Registered Entity has selected and prioritize by risk and available SPP RE resources
Evaluation of Design

• If the Registered Entity requests an evaluation, SPP RE will request documentation of the internal controls’ design

• Entity vs. Activity level controls
  – Entity-Level Controls: controls which are pervasive across an organization and include culture, values and ethics, governance, transparency and accountability
  – Activity-Level Controls: controls specific to a process or a function; may be manual or automated

• SPP RE will review the design of the internal controls and determine their sufficiency

• SPP RE will develop a Test Plan of the internal controls
Design Examples

• Preventative Controls
  – Documented process
  – Training
  – Change management
  – Log review roles and responsibilities

• Detective Controls
  – Periodic verification
  – Periodically test monitoring
Evaluation of Effectiveness

- Testing is based on the facts and circumstances of the internal control program
- Testing may include documentation such as logs, videos, software files, process checklists, etc.
- The criteria in the *ERO Enterprise Internal Control Evaluation Guide* will be used to determine the effectiveness of the implementation of the internal controls
Level of Implementation

• **Fully Implemented** – Sufficient evidence and/or affirmations are present and judged to be adequate to demonstrate process and implementation. No weakness noted.

• **Largely Implemented** - Sufficient evidence and/or affirmations are present and judged to be adequate to demonstrate process and implementation. One or more weaknesses noted.

• **Partially Implemented** – Data indicates the process and internal controls are implemented and some data indicate the practice is not implemented.
Level of Implementation

- **Not Implemented** – Some or all data are absent or judged to be inadequate; data supplied does not support the conclusion that the process is implemented. One or more significant weaknesses.

- **Missing** – The design of the control is not ready to be implemented.
Results

• After the level of implementation of controls has been determined, SPP RE will consider whether testing may be reduced during the monitoring fieldwork
  – No fieldwork
  – Reduced sampling
## Audit Testing In The Field Stage

<table>
<thead>
<tr>
<th>Internal Control Implementation Level</th>
<th>Level of Risk of Requirement (Inherent Risk Assessment)</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Low Risk Requirement Low Cyber Assets</td>
</tr>
<tr>
<td></td>
<td>Medium Risk Requirement Medium Cyber Assets</td>
</tr>
<tr>
<td></td>
<td>High Risk Requirement High Cyber Assets</td>
</tr>
<tr>
<td>Fully Implemented</td>
<td>No fieldwork</td>
</tr>
<tr>
<td></td>
<td>No fieldwork</td>
</tr>
<tr>
<td></td>
<td>Reduced testing (whole process)</td>
</tr>
<tr>
<td>Largely Implemented</td>
<td>No fieldwork</td>
</tr>
<tr>
<td></td>
<td>Reduced Testing (Gap Focus)</td>
</tr>
<tr>
<td></td>
<td>Reduced whole process testing and NERC Sampling of the Gap</td>
</tr>
<tr>
<td>Partially Implemented</td>
<td>Reduced Testing (gap focus)</td>
</tr>
<tr>
<td></td>
<td>NERC Sampling</td>
</tr>
<tr>
<td></td>
<td>NERC Sampling</td>
</tr>
<tr>
<td>Not Implemented</td>
<td>NERC Sampling</td>
</tr>
<tr>
<td></td>
<td>NERC Sampling</td>
</tr>
<tr>
<td>Missing</td>
<td>NERC Sampling</td>
</tr>
<tr>
<td></td>
<td>NERC Sampling</td>
</tr>
</tbody>
</table>
Inherent Risk Assessment and Internal Control Evaluation Timeline

- IRA started at approx 180 days prior to monitoring activity.
- IRA completed and approved at approx 165 days prior to monitoring activity and the IRA Letter is sent to the registered entity.
- The Registered Entity will provide documentation and SPP RE will evaluate the design of the Internal Control.
- Upon receiving the IRA Letter, the Registered Entity will have 10 days to request an ICE.
- The Registered Entity will provide documentation and SPP RE will evaluate the effectiveness of the Internal Controls.
- SPP RE will send the Registered Entity the monitoring activity notification at 90 days as stated in the RoP.

Timeline:
- IRA started at approx 180 days prior to monitoring activity.
- IRA completed and approved at approx 165 days prior to monitoring activity and the IRA Letter is sent to the registered entity.
- The Registered Entity will provide documentation and SPP RE will evaluate the design of the Internal Control.
- Upon receiving the IRA Letter, the Registered Entity will have 10 days to request an ICE.
- The Registered Entity will provide documentation and SPP RE will evaluate the effectiveness of the Internal Controls.
- SPP RE will send the Registered Entity the monitoring activity notification at 90 days as stated in the RoP.
References

• ERO Enterprise Inherent Risk Assessment Guide
• ERO Enterprise Internal Control Evaluation Guide
• Risk Elements Guide for Development of the 2015 CMEP IP
  – NERC Implementation Resources
  – SPP RE Assessment Questionnaire
Documents

- Acme Assessment
- Acme Assessment Letter
- ICE Workbook summary
James Williams
Lead Compliance Specialist
501.614.3261
jwilliams.re@spp.org
Comprehensive Mitigation

May 21, 2013

Jenny Anderson
Compliance Engineer - CIP
janderson.re@spp.org
501.614.3299
Goals and Benefits of Mitigation

Mitigation is intended to lessen the risk of unintended consequences and reduce vulnerabilities that may pose risk to the BES, with the ultimate goal of improving system reliability.
Submitting Comprehensive MPs

- Saves time and resources
- Speeds up mitigation and violation processing
- Could reduce the penalty amount
- Allows you to “tell your story”
The Life of a Mitigation Plan

1. Identified
2. Validated
3. Scoped
4. Status Reported
5. Changes Implemented
6. Changes Planned
7. Evidence Provided
8. Completed
9. Verified
Section 1

MITIGATION PLANNING
Mitigation Planning

• Review documentation
  – Violation Description
  – Audit Report, Self-Report, etc.
  – Evidence
  – Standard and Requirement
  – Compliance Application Reports
  – Request For Information/responses

• Determine scope
Violation Cause and Identification

- Cause
- Identification Method
- Duration
- Scope
- Standard
- Requirement
- Sub requirement(s)
Brief Summary Examples

• LACKING
  “Patch management program was not followed.”

• GOOD
  “Several patches were not assessed for applicability within 30 days.”

• BETTER
  “It was identified that 12 of 27 patches released between April 1 and April 30, 2011 were not assessed for applicability within the 30 days prescribed in CIP-007-3 R3.”
Cause and Identification

BEST

“The SPP RE audit team found at the February 2012 CIP audit that 12 of 27 patches released between April 1 and April 30, 2011 were not assessed for applicability within the 30 days prescribed in CIP-007-3 R3, R3.1.”
Violation Description

A “gold star” violation summary contains

– Standard and Requirement(s) violated
– Specific violation
– Method of identification
– Scope and duration
Relevant Information

- Root Cause
- Additional Information
Relevant Information Examples

• LACKING

“Patches were assessed.”

• GOOD

“The missed patches were assessed 38 days after availability.”

• BETTER

“These patches were not assessed in the required 30 days because the patch management program that alerts IT staff when a patch is available had become unresponsive. This was found and fixed, and the missed patches were assessed 38 days after availability.”
Relevant Information

BEST

“The patch management application alerts IT staff when a patch is available. However, the patch management application had become unresponsive and no alerts of available patches were received by IT staff. This was discovered by IT staff when they became suspicious of the lack of alerts, the patch management program was immediately restarted. The missed patches were assessed 38 days after release.”
Plan Details and Additional Information

• Tasks or actions taken or to be completed
Plan Detail Examples

• LACKING

“Patches were assessed.”

• GOOD

“The patch management program was restarted, and the missing patches were assessed.”

• BETTER

“The patch management program was restarted, and the missed patches were assessed 38 days after availability and have been applied.”
Plan Details

BEST

“Immediately upon realizing the patch management application had failed, IT staff restarted the application on April 9, 2013 and inventoried those patches that were not assessed/applied. The 12 missed patches were assessed the same day; 38 days after their availability. These patches were subsequently installed. A second patch management server will be installed and configured to mitigate the risk of issue with either.”
Additional Information Examples

• BAD

• GOOD

“Staff are taking measures to improve the patch management program.”

• BETTER

“IT Staff will install a second patch management server.”
“A backup patch management server will be installed and configured to mitigate any future issues with the primary. Until then, IT staff will manually verify the patch management program is functioning.”
Plan Details and Additional Information

**PLAN DETAILS**

- Corrective action(s)
- Mitigating action(s) taken
- Actions to be taken

**ADDITIONAL INFO**

- Any compensating measure(s)
- Other actions taken or planned

- Able to be supported by evidence
Activities and Timeline

- Future milestones
- Supported by evidence
Milestones

Should be:

• Multiple
• Future dated – any completed activity should be documented in the plan details section
• Stepped activity, i.e. 1\textsuperscript{st}, 2\textsuperscript{nd}, 3\textsuperscript{rd}
• Able to be supported by evidence
Milestones

BAD

• Single milestone
• Are complete
• Are not relevant
• Cannot be supported by evidence

BETTER

• Future activity
• Multiple
• Specific
• Stepped
• Able to be supported by evidence
Milestone Examples

GOOD

• Install and configure secondary patch management server

BETTER

• Install and configure secondary patch management server

• Test patch notifications scenarios including outage of either server

• Place secondary patch management server in production
Milestones

“Gold star” milestones

• Are appropriate to the violation
• Corrective or mitigating action
• Consider evidence
**Proposed Completion Date**

- When all activities in the mitigation plan were or will be completed
- The final milestone proposed completion date
- The proposed and actual completion dates should be consistent
Reliability Risk and Prevention

**Risk**

Potential Impact to: Entity Neighbors BES

**Prevention**

Immediate Future

---

*Reliability Risk* While the Mitigation Plan is being implemented, the reliability of the bulk Power System may remain at higher Risk or be otherwise negatively impacted until the plan is successfully completed. To the extent they are known or anticipated: (i) Identify any such risks or impacts, and; (ii) discuss any actions planned or proposed to address these risks or impacts:

*Prevention* Describe how successful completion of this plan will prevent or minimize the probability further violations of the same or similar reliability standards requirements will occur:

Describe any action that may be taken or planned beyond that listed in the mitigation plan, to prevent or minimize the probability of incurring further violations of the same or similar standards requirements:
Risk Statement Examples

• **LACKING**
  “There is no risk.”

• **GOOD**
  “There is minimal risk because we are small and patches are rarely released that have a serious impact.”

• **BETTER**
  “There is minimal risk to the BES because the patches released were not all urgent, and because the systems for which patches were released were protected by other means.”
Risk Statement

BEST

“There was minimal risk to the BES because none of the vulnerabilities for which the patches were released were exploited, and no attempt to do so was identified at the firewall or intrusion detection system. Of the 12 patches not assessed, all were for Windows systems, but only two were security patches; the others were optional updates with no security risk. The security patches were for vulnerabilities in Internet Explorer; only two CAs in the ESP run IE, and these are both further protected with up-to-date anti-virus and anti-malware software.”
Risk Statement

A “gold star” risk statement

- Actual AND potential risk to the BES
- Considers “what ifs”
- Compensating measures
- Mitigation of risk during the plan
- Mitigation of risk by the plan
Prevention Statement Examples

• LACKING

“Completion of the plan will minimize or prevent further occurrences.”

• GOOD

“The 30 day patch assessment requirement will not be missed.

• BETTER

“By eliminating the risk of missing the 30 day patch assessment, patches will be assessed per the requirement and applied with the intended urgency.”
Prevention Statement

BEST

“By implementing a redundant patch management system, the risk of missing the 30 day patch assessment will be eliminated and patches will be assessed per the requirement and applied with the intended urgency.”
Prevention Statement

A “gold star” prevention statement tells how the entity will prevent further or similar violations and addresses

– Root cause
– Future considerations
– Compensating measures
– Mitigation of risk during the plan
– Mitigation of risk by the plan
Section 1

COMPLETING MITIGATION
Evidence

Evidence should

- Be submitted for all plan details/milestones
- Be specific to the activity
- Provide a supportable end date
- Be quality
Evidence Submission

CDMS

- For evidence that does not contain sensitive CIP-related information

EFT Server

- CIP-protected or sensitive information
- Requires access
- Is secure
Determining What to Submit

1. Violation Description and Relevant Information
2. Plan details and Additional Information
3. Activities and Timeline (Milestones)
4. Risk and Prevention Statements
Examples of Evidence

- Change record of the application restart
- Patch inventory and assessment
- Purchase orders/change records
- Testing records
Certification of Completion

Submit only when mitigation plan is complete AND MP has been reviewed to determine that it

– Meets the Standard and Requirement
– Provides sufficient supporting date of completion of milestones and plan
Certification of Completion

Submit only when mitigation plan is complete AND MP has been reviewed to determine that it

– Meets the Standard and Requirement

– Provides sufficient supporting date of completion of milestones and plan

– Was completed in advance of or on the proposed completion date
Submitting Comprehensive MPs

- Saves time and resources
- Speeds up mitigation and violation processing
- Could reduce the penalty amount
- Allows you to “tell your story”
Mitigating Activities for Registered Entities

Registered Entities may now submit Mitigating Activities for self-reported compliance issues or during self certification when the Entities have completed mitigation. This option is available to Entities on the Self Report Detail screen:

Select “Mitigating Activities from the Selection Links on the left of the Self Report Detail entry screen.

To submit Mitigating Activities, mitigation must be complete and any preventative measure(s) must be in place at the time of submission of the self report or non-compliant self certification for which a compliance issue has not been previously reported. All mitigating activities and the preventative measure(s) should be detailed in the Self Report screen:
Enter all mitigation and the preventative measure(s) in place to prevent reoccurrence of the issue. Once Mitigating Activities have been submitted for a self report or non-compliant self certification, these cannot be changed/reopened.

Enter the completion date:

Enter the date all mitigating activities were complete and preventative measures were in place to reduce the risk of reoccurrence of the issue. This date must be in the past, and all activities must be able to be confirmed as complete to submit Mitigating Activities.
Submit evidence of completion and prevention along with the Mitigating Activity Affadavit in the Entity Documents:

The Mitigating Activities will be reviewed as part of the triage process by the Enforcement Staff, and if it is determined that the mitigating activities meet the requirements, a Mitigation Plan will not be required. However, if it is determined that mitigation is not complete or is not supported by the evidence provided by the Registered Entity, the Enforcement Staff will require the Entity to submit a Mitigation Plan.

Submit Mitigating Activities

- When mitigation is complete and prevention of recurrence is in place
  - With a completion date in the past
- With evidence supporting that Mitigating Activities were complete by the completion date
  - With a Mitigating Activity Affadavit
Definition – Unresolved Maintenance Issue

- A deficiency identified during a maintenance activity that causes the component to not meet the intended performance, cannot be corrected during the maintenance interval, and requires follow-up action.

- The entity “shall demonstrate efforts to correct any identified Unresolved Maintenance Issues.”
Unresolved Maintenance Issues (UMI)

Evidence

- List of Unresolved Maintenance Issues
  - April 1, 2015
    - Any UMI on this date will be reviewed back to 2014
    - Tracking from April 1, 2014 for UMI will be needed
  - List is to include
    - Resolved Maintenance Issues
    - Remaining Unresolved Maintenance Issues
Transition

• While in transition, be prepared to identify:
  o All applicable Protection System components.
  o The plan under which they were last maintained; PRC-005-2 or the applicable Legacy plan.
Transition

Maintain documentation to demonstrate compliance with the Legacy Standards

- until the **entity meets the requirements** of PRC-005-2 in accordance with this implementation plan.
Implementation

PRC-005-2 was effective April 1, 2014

- Enforcement Date in U.S.:
  - April 1, 2015 (R1, R2, R5)
- Must have a Protective System Maintenance Program (Time Based Maintenance, Performance Based Maintenance or both).
- Phased implementation based on maximum allowable interval.
- Enforcement Date: October 1, 2015 (R3, R4)
- Retire Legacy Standards by April 1, 2027

Implementation Plan
Implementation

• Each entity will maintain each of their Protection System components according to their maintenance program already in place for the legacy standards or according to the program for PRC-005-2, but not both.

• Once an entity has designated PRC-005-2 as its maintenance program for specific Protection System components, they cannot revert to the legacy program for those components. *(You get to make the call, but you can’t take it back.)*

• New components after April 1, 2015 must be in the PRC-005-2 program.
## Implementation Timetable

<table>
<thead>
<tr>
<th>Max. Maintenance Interval</th>
<th>% Compliant</th>
<th>By</th>
</tr>
</thead>
<tbody>
<tr>
<td>Less than 1 year</td>
<td>100%</td>
<td>Oct. 1, 2015</td>
</tr>
<tr>
<td>1-2 calendar years</td>
<td>100%</td>
<td>Apr. 1, 2017</td>
</tr>
<tr>
<td>3 calendar years</td>
<td>30%</td>
<td>Apr. 1, 2016</td>
</tr>
<tr>
<td>3 calendar years</td>
<td>60%</td>
<td>Apr. 1, 2017</td>
</tr>
<tr>
<td>3 calendar years</td>
<td>100%</td>
<td>Apr. 1, 2018</td>
</tr>
<tr>
<td>6 calendar years</td>
<td>30%</td>
<td>Apr. 1, 2017</td>
</tr>
<tr>
<td>6 calendar years</td>
<td>60%</td>
<td>Apr. 1, 2019</td>
</tr>
<tr>
<td>6 calendar years</td>
<td>100%</td>
<td>Apr. 1, 2021</td>
</tr>
<tr>
<td>12 calendar years</td>
<td>30%</td>
<td>Apr. 1, 2019</td>
</tr>
<tr>
<td>12 calendar years</td>
<td>60%</td>
<td>Apr. 1, 2023</td>
</tr>
<tr>
<td>12 calendar years</td>
<td>100%</td>
<td>Apr. 1, 2027</td>
</tr>
</tbody>
</table>
Internet
Join the **SPPGuest** network. Open your internet browser and enter your email address (no password required) on the Guest User page.

Restrooms & Vending Machines
From the auditorium, go left, then left again at the next hallway.

More restrooms are behind the atrium stairway.

Break Room with Tables
Other side of the vending machine wall

Designated Smoking Area
Outside the large break room

Business Center
Behind the reception desk. Ask a staff member for assistance with copies or faxes. A PC and printer is available.
Watch 37 “SPP RE Basics” videos!

- Mock 693 Audit
- NetAPT Demo
- Self-Reporting: When and How
- Standards: How to Read & Understand
- TFE Expectations and Issues
- Training Employees on Compliance

STANDARDS - HOW TO READ & UNDERSTAND

SPP.org > Regional Entity > Outreach
2014 SPP RE Year in Review

• Achieved 122% of 2014 staff goals and metrics

Numbers at a Glance

- Audit reports issued: 54
- Audits performed: 56
- Events processed: 30
- FFTs processed: 62
- Mitigation Plans reviewed: 101
- Newsletters published: 12
- Registration changes: 25
- Reliability Assessments published: 3
- TFE actions: 271
- Videos produced: 8
- Violations processed: 188
- Violations received: 121
- Workshop & webinar attendees: 578
BES Definition Implementation

- 134 exclusion self-determinations and 8 inclusion self-determinations filed by SPP RE entities
- 996 self-determinations filed NERC wide
- 3 exception requests for exclusion have been filed at SPP RE – 11 NERC-wide
- BESnet tool still available for use
  - Contact Greg Sorenson for additional information
Vegetation Management Update

- NERC 4Q 2014 Vegetation Management Report
  - No reportable contacts in SPP RE footprint
  - 7th consecutive quarter with no reportable contacts
NERC Facility Ratings Alert Status

• Final reports were due to SPP RE by January 15
• Interim reports, for those with approved extensions, were also due January 15
• Program is winding down – all entities should either be finished or have an approved extension
SPP RE Regional Events - 4Q 2014

• Four Category 1 and Two Category 2 events were analyzed
  – 1 Category 1h - Loss of monitoring or control at a control center
  – 1 Category 1f. Unplanned evacuation from a control center
  – 2 Category 1a-An unexpected outage, contrary to design that results in three or more BPS facilities.
  – 2 Category 2b- Complete loss of SCADA for 30 minutes

• YTD 30 total events
  – 27 of 30 events have been rated Category 0 or Category 1
SPP RE Misoperation Report as of 3Q 2014
# Most Violated Standards

Based on rolling 12 months through 12/31/14 [Represents ~ 88% of total violations]

<table>
<thead>
<tr>
<th>SPP RE Rank</th>
<th>NERC 12 Month Rank *</th>
<th>Standard</th>
<th>Description</th>
<th>Number of Violations</th>
<th>Risk Factor</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>1</td>
<td>CIP-007</td>
<td>Systems Security Management</td>
<td>28</td>
<td>Med./Lower</td>
</tr>
<tr>
<td>2</td>
<td>3</td>
<td>CIP-005</td>
<td>Electronic Security Perimeters</td>
<td>15</td>
<td>Med./Lower</td>
</tr>
<tr>
<td>3</td>
<td>2</td>
<td>CIP-006</td>
<td>Physical Security - Critical Cyber Assets</td>
<td>13</td>
<td>Med./Lower</td>
</tr>
<tr>
<td>4</td>
<td>10</td>
<td>FAC-008</td>
<td>Facility Ratings (includes FAC-009)</td>
<td>11</td>
<td>Med./Lower</td>
</tr>
<tr>
<td>5</td>
<td>6</td>
<td>CIP-003</td>
<td>Security Management Controls</td>
<td>11</td>
<td>Med./Lower</td>
</tr>
<tr>
<td>6</td>
<td>7</td>
<td>CIP-002</td>
<td>Critical Cyber Asset Identification</td>
<td>8</td>
<td>High/Lower</td>
</tr>
<tr>
<td>7</td>
<td>4</td>
<td>CIP-004</td>
<td>Personnel &amp; Training</td>
<td>8</td>
<td>Med./Lower</td>
</tr>
<tr>
<td>8</td>
<td>8</td>
<td>VAR-002</td>
<td>Network Voltage Schedules</td>
<td>6</td>
<td>Med./Lower</td>
</tr>
<tr>
<td>9</td>
<td>5</td>
<td>PRC-005</td>
<td>Protection System Maintenance</td>
<td>4</td>
<td>High/Lower</td>
</tr>
<tr>
<td>10</td>
<td>**</td>
<td>TOP-002</td>
<td>Normal Operations Planning</td>
<td>2</td>
<td>Med./Lower</td>
</tr>
</tbody>
</table>

* NERC as of June 30, 2014
** Not in NERC Rolling 12 month Top Ten
Violations by Year

![Graph showing violations by year with data points for years 2009 to 2014, including projected data for 2014. The graph compares ERO Total and SPP RE.]
2015 Outreach

• **Workshops**
  June 2-3, CIP 2015 Workshop, Kansas City  [Register](#)
  Sept. 29-30, Fall 2015 Workshop, Dallas  [Register](#)
  Workshops are followed by RTO Compliance [Forums](#)

• **Webinars**
  April 6, Summer Reliability Assessment, 2:30-3:00  [Register](#)

• **Trustee Meetings**
  April 27, 2015 - Tulsa
  June 15, Teleconference (budget meeting)
  July 27, 2015 - Kansas City
  October 26, 2015 - Little Rock