NERC Compliance Workshop
Chicago, June 21, 2011
A Reliable Bulk Power System

NERC. Reliability. Accountability.

T.J. Galloway
Sr. Vice President and Chief Reliability Officer
June 21, 2011, NERC Compliance Workshop
ERO: A Unique Form of Regulation
different than government or self-regulation

- Unique industry perspective
  - Real-time interconnectedness of power systems
  - Cost of unreliable service affects all
  - Active industry involvement in solving problems

- Unique regulatory model
  - Independent board governance at ERO
  - Mandatory standards developed by industry
  - Rigorous monitoring/audit program
  - Oversight by U.S. and Canadian authorities
Five Key Success Factors for building a foundation of public trust

- Risk-based approach, with reliability performance measurably improving
- Reliability-learning, self-correcting industry
- Culture of compliance, enforcement backstop
- Commitment to security/resilience of grid
- Positive ERO relationships and reputation
  - Leading expert organization for grid reliability
  - Trusted leader and advocate for reliability
  - Effective relations with U.S. and Canadian authorities
Reliability Risk Management Concept

Event Driven
Severity Risk Index (SRI)
Measures Risk from System Events

Condition Driven
Portfolio of Reliability Indicators
Seasonal & LTRA
Monitoring Risk from System Conditions

Standards/Statute Driven
Violation Risk Index (VRI)
Measures Risks from Known Unmitigated Violations

Cornerstone of risk-management concepts

Severity

Avoid

Learn and Reduce

Inverse Cost-Benefit

Reporting Threshold

Frequency
NERC CEO Current Risk Priorities

- Mis-operations of relay and controls systems
- Human errors by field personnel
- Ambiguous, incomplete voice communications
- Right-of-way maintenance and clearances
- Changing resource mix
- Integration of new technologies
- High impact, low frequency events
- Cyber security vulnerabilities
Reliability Standards

- Results – based standards
- Standards process timeliness and accountability
  - Industry
  - Process improvements
  - Governance (Standards Oversight & Technology Comm)
- Standards prioritization
- Addressing standards directives
- Standards clarifications and interpretations
- BES definition and adequate level of reliability
Compliance

- Risk-based approaches
  - Risk drivers for monitoring
  - Penalties, remediation, record proportional to seriousness
  - Internal Compliance Program
    - Focus on effective internal controls prevention
    - Effective incentives to promote compliant behaviors
    - Culture of Compliance

- Performance-based adjustments
- Transparency of process and expectations
Enforcement

- ERO conclusions upheld
- NOPs as key information source
- Efficiency / throughput
  - Record proportionality
  - Administrative Citation Process
  - Other
- Value of:
  - Strong internal compliance programs
  - Timely mitigation
Event Analysis and Investigations

- Process-driven event review
  - Screening and triage
  - What happened?
  - Why did it happen (root cause analysis)
  - Lessons learned made transparent

- Regions and registered entities part of process and key to success
  - Learning, self-correcting industry
  - Correct incentives
Critical Infrastructure Resilience

- Multifaceted approach to mitigate risk
  - Standards protect critical assets
  - Alerts provide rapid response and impact mitigation for vulnerabilities
  - Preparedness and recovery
  - Long-term design, hardening solutions

- Develop government interface to produce actionable information for industry

- Communicate results to government and public
ERO Model is Working and Will Work

execution is better with effective communications

- Policy level discussions
  - July 6, 2010 conference on standards
  - November 18, 2010 conference on compliance
  - February 8, 2011 reliability summit
- Setting of direction and priorities
- Constructive dialog and consultation
Contributions Needed from Industry

- Delivery of priority, results-based standards
- Strive for compliance excellence (lean in)
- Engage in event analysis and lessons learned
- Promote/support risk-based, learning approach
- CEO/executive engagement
Risk Based Reliability Compliance Monitoring and Entity Assessment

Michael Moon
Director of Compliance Risk Management
June 21, 2011, NERC Compliance Workshop
Agenda

- Risk Based Compliance Monitoring and Reliability
- Entity Assessment and Accountability

111 Reliability Standards
1274 Requirements
Authority and Responsibility

- NERC is the FERC-certified Electric Reliability Organization (ERO), along with the Regional Entities, are accountable to the:
  - Regulators
  - Industry
  - Public

- Statutory Functions:
  - Reliability Assessments
  - Standards Development with industry
  - Compliance Monitoring and Enforcement
Basis for a risk based approach:

- Auditing and compliance monitoring do not guarantee compliance and reliability
- Auditing provides reasonable assurance of compliance
- Audit scope can and should take into account the entities internal compliance program
## Risk Based Reliability Compliance Monitoring

**Where we have come from:**

<table>
<thead>
<tr>
<th>Actively Monitored List</th>
<th>Number of Reliability Standards</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Year</td>
</tr>
<tr>
<td>Compliance Audit</td>
<td></td>
</tr>
<tr>
<td>Self-Certification</td>
<td></td>
</tr>
<tr>
<td>Periodic Data Submittals</td>
<td></td>
</tr>
<tr>
<td>Exception Reporting</td>
<td></td>
</tr>
<tr>
<td>Spot Check</td>
<td></td>
</tr>
<tr>
<td>Subject to Compliance Investigation</td>
<td></td>
</tr>
<tr>
<td>Subject to Self-Reporting</td>
<td></td>
</tr>
<tr>
<td>Subject to Complaint</td>
<td></td>
</tr>
</tbody>
</table>
A refined risk based, informed compliance monitoring program to:

- Enhance reliability
- Focus on a core set critical reliability standards
- Provide predictability for the industry to develop compliance programs
- Manage resources effectively and efficiently
- Provide flexibility to react to emerging trends
Criteria for Selection of Standards Audited for the 2011 Actively Monitored List:

- NERC top 20 list of allegedly violated reliability standards
- High Violation Risk Factor (VRF)
- Violation Risk Index (VRI)
- Identified in past events and major reliability issues
- Input from Regional Entities
- Assessment of Entities Internal Compliance Program and Compliance Culture
Criteria for Selection of Standards Audited for the 2012 Actively Monitored List:

- Build on the 2011 analysis
- Consider the current top reliability risks
- Continued flexibility for the Regional Entities
- Provide longer horizon and predictability for compliance program management
- Field trial audits of standards still in the implementation plan phase
- Review the CIP standards and adjust AML as appropriate
Top Reliability Risk Priorities:

- Mis-operations of relay and controls systems
- Human errors by field personnel
- Ambiguous, incomplete voice communications
- Right-of-way maintenance and clearances
- Critical Infrastructure Protection
- Changing resource mix
- Integration of new technologies
- High impact, low frequency events
## 2012 Implementation Plan and AML

### Where we are going:

#### Applicable 693 Requirements by Year

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>BA</td>
<td>61</td>
<td>137</td>
<td>107</td>
<td>175</td>
<td>95</td>
<td></td>
</tr>
<tr>
<td>GO</td>
<td>53</td>
<td>74</td>
<td>34</td>
<td>47</td>
<td>40</td>
<td></td>
</tr>
<tr>
<td>GOP</td>
<td>19</td>
<td>70</td>
<td>23</td>
<td>34</td>
<td>9</td>
<td></td>
</tr>
<tr>
<td>LSE</td>
<td>8</td>
<td>42</td>
<td>8</td>
<td>22</td>
<td>9</td>
<td></td>
</tr>
<tr>
<td>RC</td>
<td>54</td>
<td>127</td>
<td>93</td>
<td>127</td>
<td>72</td>
<td></td>
</tr>
<tr>
<td>TO</td>
<td>77</td>
<td>103</td>
<td>70</td>
<td>86</td>
<td>86</td>
<td></td>
</tr>
<tr>
<td>TP</td>
<td>49</td>
<td>83</td>
<td>51</td>
<td>86</td>
<td>86</td>
<td></td>
</tr>
<tr>
<td><strong>Avg Reqs per Function</strong></td>
<td><strong>36</strong></td>
<td><strong>61</strong></td>
<td><strong>38</strong></td>
<td><strong>55</strong></td>
<td><strong>42</strong></td>
<td><strong>24</strong></td>
</tr>
</tbody>
</table>
Entity assessment components to determine audit scope and compliance monitoring:

- Technical and Risk Profile
- Reliability Performance
- Internal Compliance Program and Culture
- Compliance History
- Regional Entity Perspective / Analysis
Entity Assessment

- Technical and Risk Profile
  - Company’s size and structure
  - Registered Functions
  - Footprint and interconnections
  - Generation capacity
  - Nuclear Generation capacity
  - Transmission capacity
  - Points of interconnection
Entity Assessment

- Reliability Performance
  - Metrics provide a quantitative approach for measuring a Registered Entity’s performance.
  - Consistent metrics yield a baseline to compare performance as well as measure performance from a previous year.
  - Generation Availability Data System
  - Transmission Availability Data System
  - Events data
  - Geographic or regional challenges
Entity Assessment

- Internal Compliance Program and Culture
  - An internal compliance program is critical for the entity and for a risk based approach to compliance monitoring
  - Self-monitor reliability and compliance
  - Internal controls
  - Corrective action programs
  - Self reporting as necessary
  - Culture of compliance
Entity Assessment

- Compliance Metrics and History
  - Open enforcement actions
  - Discovery Method
  - Mitigation Plan
  - Consideration of the facts and circumstances
- Status of any open mitigation plans.
- Violation history
  - Method of Discovery
  - Repeat violations
Entity Assessment

- Regional Entity Perspective / Analysis
  - Qualitative assessment
  - Regional and geographic challenges
  - Interconnection challenges
Summary:

- Risk Based Reliability Compliance Monitoring is critical to:
  - Manage resources
  - Focus compliance
- Entity Assessment is an essential component of Risk Based Reliability Compliance Monitoring
Questions
Internal Compliance Programs (ICP)

Val Agnew
Manager of Interface and Outreach
June 21, 2011, NERC Compliance Workshop
Purpose

To provide additional information regarding:

• Importance of ICPs
• How an ICP is reviewed
• Types of evidence/information to provide to a Regional Entity
Discuss purpose and importance of ICPs

Examine each of the 13 questions
  • Discuss common deficiencies
  • Review the Internal Compliance Program of two large entities for each of the questions

Discuss a summary of the 2 example ICPs

Discuss the additional FERC considerations for an ICP review during a 1.b investigation
Importance of an ICP

- **Internal Compliance Program**
  - Not required by a standard; Registered Entity “Leaning in” for reliability
  - Internal Controls
  - Corrective Action Program, including effective incentives to promote compliant behaviors
  - Culture of Compliance

- **Risk and Performance-based Compliance Monitoring**
  - Audit scope based on entity’s performance
Registered Entity Assessment

- Number of violations discovered via audit or investigation
- Number of repeat violations
- Mitigation plans
- Number of events analysis
- Number of investigations
- Results and cooperation of prior compliance monitoring methods
- Previous enforcement actions
- **Assessment of culture of compliance, internal controls and corrective action plans (ICP)**
- Consideration of what an entity is doing well vs. poorly
Evaluation in an Enforcement Action

- Influence on an assessed penalty
  - Demonstrates Culture of Compliance
  - Determination of violation history

- Objective is to resolve issues at the root of the non-compliance
  - Where did the ICP originate?
  - What registered entities does the ICP cover, or
  - Which registered entities have adopted the ICP?
    - Same management or implementation
Evaluating an ICP

- Evaluations of the ICPs by the Regions is maturing
  - Timing
  - Voluntary
  - On-site vs. Off-site audits

- All Regions moving toward evaluations of ICPs based on the FERC “13 questions” provided in the 2005 orders
FERC Orders

- Policy Statement on Enforcement *(13 questions)*
  - Docket No. PL06-1-000, 113 FERC ¶ 61,068 (October 20, 2005)

- Revised Policy Statement on Enforcement
  - Docket No. PL08-3-000, 123 FERC ¶ 61,156 (May 18, 2008)

- Policy Statement on Compliance *(4 Hallmarks)*
  - Docket No. PL09-1-000, 125 FERC ¶ 61,058 (October 16, 2008)

- Policy Statement on Penalty Guidelines
  - Docket No. PL10-4-000, 130 FERC ¶ 61,220 (March 18, 2010)
  - suspended on April 15, 2010

- Revised Policy Statement on Penalty Guidelines *(Additional criteria during a FERC 1.b investigation)*
  - Docket No. PL10-4-000, 132 FERC ¶ 61,216 (October 17, 2010)
The first Policy Statement on Enforcement following the Energy Policy Act of 2005

FERC recognized the importance of internal compliance and cooperation

Is the base order that outlined the “13 questions” still used for evaluation of internal compliance programs

Internal compliance programs are also addressed in the GAGAS (Yellow Book), Chapter 7
Consolidated 13 questions into “4 Hallmarks” of effective compliance practices:

- Senior management leadership
- Preventive measures in place
- Prompt detection, cessation, and self-reporting
- Effective remediation

No one model

- Company is in best position to assess risks and devise appropriate compliance practices
Question 1

- Does the company have an established, formal program for internal compliance?
  - Signature, Title, Date
  - Is it signed by a senior officer?
  - Does it grant authority and responsibilities for the ICP?
  - Does the document have version control?
Question 1
Does the company have an established program?

Entity A

- The entity’s ICP consists of three tiers and multiple documents:
  - Corporate Level Ethics Code
  - Corporate Policies and Procedures
  - Operating Manual for Electric Reliability Standards
- How the three tiers of documents tie together is not clear.
- The documents are not signed, but identify the senior officer that approved the document.
- All documents meet the remainder of the criteria.

Entity B

- The entity’s ICP consists of three tiers and multiple documents
  - Corporate Policy
  - Compliance Assurance Program
  - Individual Department Procedures

✓ The documents are presented as a package.
- The documents are not signed, but identify the senior officer that approved the document.
- All documents meet the remainder of the criteria.
Question 2 – Entity A

Is the ICP well documented and widely disseminated?
Question 2 – Entity B

Is the ICP well documented and widely disseminated?

- Corporate Policy for Compliance with Reliability Standards
  - Corporate Procedure: Compliance Assurance Program
    - CIP Security Policy
      - Security Procedures
      - Coordination for 693 Standards
        - Compliance Monitoring
        - Compliance Self-Assessment
        - Assurance of Affiliate Compliance
        - Investigation of Possible Non-Compliance
Is the ICP well documented and widely disseminated within the company?

- Dissemination should be throughout the organization, not just compliance
- Common Deficiency – lack of dissemination throughout entire organization, such as HR, Legal, Executive, Accounting, etc.
- Does the ICP identify when, where and to whom it was disseminated?
Question 2
Is the ICP well documented and widely disseminated?

Entity A

- Where ICP was posted and accessible by employees was not disclosed
- Fragmented
- ICP is disseminated through training
- Compliance Communications are issued to support the ICP and notify employees of changes

Entity B

- The entity’s ICP is posted on the entity’s intranet for employee accessibility
- Cohesive and organized
- ICP is disseminated through training
- The entity has a staff dedicated to monitoring changes in the standard and notifying effected managers
Question 3

- Is the program supervised by an officer or other high-ranking official?
  - Oversight position clearly identified including responsibilities
  - Reflected in an Organizational Chart
  - Common Deficiency - inconsistency of the named oversight position or titles in the Organizational Chart, the ICP, and the responses to 13 questions
Question 3

Is the program supervised by a high-ranking official?

Entity A
- Supervised by Executive Vice President of Operations
- The entity established a Corporate Compliance Committee, which approves the authority of the VP of Operations, and includes a VP of Ethics and Compliance (Compliance Manager)
- Organizational Chart not provided

Entity B
- Supervised by Senior Vice President of Operations
- The entity established a Regulatory Compliance Committee and has named a Corporate Compliance Officer for reliability standards (Compliance Manager)
- No Organizational Chart was provided; organizational structure was described
Question 4

- Does the compliance official report to or have independent access to the Chief Executive Officer and/or the Board of Directors?
  - The ICP needs to specifically identify how and when the oversight position has access to the CEO/Board
  - Common Deficiency - there is no independent access to the CEO/Board, or it is not identified on the Organizational Chart or stated in the ICP
Question 4

Does official have independent access to CEO or Board?

**Entity A**
- The VP of Ethics and Compliance reports directly to the Executive Vice President and General Counsel
- Compliance Official is not the person that has oversight
- No Organization Chart was provided

**Entity B**
- The Chairman of the Regulatory Compliance Committee and the Corporate Compliance Officer has unrestricted access to the CEO
- Compliance Official is not the person that has oversight
- No Organization Chart was provided, however the organizational structure was described
Question 5

- Is the program operated and managed so as to be independent?
  - Independence from day to day decisions over NERC Reliability is needed
  - The ICP manager should not have responsibility over any direct implementation of a standard
  - How to achieve independence:
    - Utilize other departments such as Human Resources, Legal, or internal Auditing to operate or manage the program
    - Use other outside sources such as other related facilities or plants
Question 5
Is the program independently operated and managed?

Entity A
- The entity performs an internal audits supervised by the VP and General Auditor, who is accountable to Sr. Management and an Audit Committee
- Independence not verified

Entity B
- The entity has two divisions that are independent from the system operations and planning divisions
- Independence not verified
Entity A Perceived Organizational Chart

Corporate Compliance Committee

CEO

Independent Access to CEO

Executive VP of Operations

VP

VP

Executive VP of Ethics & Compliance

Executive VP of General Auditing

VP of General Audits

Reliability Oversight Committee (Business Unit’s Executive Management)

Business Unit

Business Unit

Business Unit

Business Unit

Cross-Functional Compliance Committee

Compliance Staff

Compliance Staff

Compliance Staff

Compliance Staff
Are there sufficient resources dedicated to the compliance program?

• An independent compliance officer is necessary to be considered fully staffed

• Are there enough resources for the entity based on its size?

• Budget should identify ICP funding
  ▪ Should be managed independently

• Common deficiency - funding/budget is not mentioned in the ICP
**Question 6**

*Are their sufficient ICP resources?*

<table>
<thead>
<tr>
<th>Entity A</th>
<th>Entity B</th>
</tr>
</thead>
<tbody>
<tr>
<td>- Staffing appears to be sufficient; there are a number of employees in each functional unit</td>
<td>- Staffing appears to be sufficient; there are a number of employees in each functional unit</td>
</tr>
<tr>
<td>- Entity stated that it provides a budget for its compliance activities, but did not provide or elaborate</td>
<td>- Entity stated that it provides a budget for its compliance activities, but did not provide or elaborate</td>
</tr>
</tbody>
</table>
Is compliance fully supported by senior management? For example, is senior management actively involved in compliance efforts and do company policies regarding compensation, promotion, and disciplinary action take into account the relevant employees’ compliance with Commission regulations and the reporting of any violations?

- The Compliance Program needs a clear description of how Senior Management is involved and must discuss how corrective actions are ensured.

- Example of participation with Senior Management:
  - Meetings on a monthly or other specified basis
  - Agenda topics such as new standards, Self Certifications, Audits, Internal Assessment status and results
## Question 7
**Is compliance fully supported by senior management?**

<table>
<thead>
<tr>
<th>Entity A</th>
<th>Entity B</th>
</tr>
</thead>
<tbody>
<tr>
<td>✓ Committee comprised of executives from each business unit meets weekly or bi-weekly to provide compliance oversight</td>
<td></td>
</tr>
<tr>
<td>- Sr. management must annually certify their business units maintain compliance processes and demonstrate due diligence in performing compliance activities</td>
<td></td>
</tr>
<tr>
<td>✓ Entity promotes and enforces its compliance program through appropriate incentives and disciplinary measures consistent with the HR policy</td>
<td></td>
</tr>
<tr>
<td>✓ Entity instituted an anonymous reporting to report concerns to senior management program</td>
<td></td>
</tr>
<tr>
<td>✓ CEO attends Mock Audits</td>
<td></td>
</tr>
<tr>
<td>✓ CEO and Board meet regularly with Reliability Compliance and Oversight committee chair and are invited to attend Reliability Compliance and Oversight meetings</td>
<td></td>
</tr>
<tr>
<td>- Sr. VP Operations reviews all self-certifications and evidence</td>
<td></td>
</tr>
<tr>
<td>✓ Entity established a corporate goal associated with reliability standards</td>
<td></td>
</tr>
<tr>
<td>✓ CEO issued a letter to all employees emphasizing importance of compliance</td>
<td></td>
</tr>
<tr>
<td>✓ Discipline addressed in Corporate Policy</td>
<td></td>
</tr>
<tr>
<td>✓ Entity instituted an anonymous reporting to report concerns to senior management program</td>
<td></td>
</tr>
</tbody>
</table>
Question 8

- How frequently does the company review and modify the compliance program?
  - ICP should clearly identify how frequently the review takes place
  - An annual review basis may not be sufficient based upon changing of Standards
    - Semi-Annual or shorter basis is best
## Question 8

**How frequently does the company review its ICP?**

<table>
<thead>
<tr>
<th>Entity A</th>
<th>Entity B</th>
</tr>
</thead>
</table>
| - Entity must review its compliance program *at least annually* by each subject matter expert for their assigned area(s)  
- Entity has implemented software to provide controls and tests to ensure compliance is maintained  
- Compliance Communications are conducted to support the ICP and notify personnel of changes | - Reliability Compliance and Oversight committee has responsibility to modify and review ICP  
- While new, review and modification are continuous  
- The entity’s Compliance Assurance Program includes an *annual review*, as a minimum, and modifications will be made on an as-needed basis  
- Entity has department dedicated to notifying applicable managers of changes |
How frequently is training provided to all relevant employees?

- The ICP should document how and when training takes place
  - Initial, refresher, and ongoing training, for example
Question 9
How frequently is training provided?

Entity A

✓ Training is conducted:
  ✓ Whenever a new employee joins company
  ✓ Whenever an employee moves jobs
  ✓ Annually or more frequently based on risk

▪ Communications come out once a month including information on a new standard

Entity B

▪ Training is provided to the staff based on their individual involvement with reliability standard activities.

▪ Training is provided on an on-going basis, specific timing was not provided

▪ Entity has a staff that communicates changes, personally and through other communication vehicles
Question 10

Is the training sufficiently detailed and thorough to instill an understanding of relevant rules and the importance of compliance?

- Detailed training should be provided to employees with direct responsibility for Reliability Standards
- Common Deficiency - high level awareness training is missing
Question 10
Is training detailed and thorough?

Entity A

- Not enough detail provided to determine

Entity B

- Training is provided in 3 tiers
  - Tier 1 = high level compliance training for all employees
  - Tier 2 = more detailed training targeted to personnel with responsibilities for developing and maintaining evidence of compliance with the standards.
  - Tier 3 = training for the retention of evidence targeted to responsible personnel
In addition to training, does the company have an ongoing process for auditing compliance with Commission regulations?

- The ICP should identify the periodicity, by whom, and how self assessments are performed
- Self assessments or audits should take place on an off cycle from regular audits or self certifications
- Keep evidence to show compliance during off cycle internal reviews
Question 11
Is there an ongoing process for monitoring compliance?

Entity A
- Periodicity was not provided and did not appear to be required, perhaps due to continuous monitoring of software tool.
- Entity has a process that provides methods for use in scheduling, planning, conducting and reporting Assessment results and a software tool that assesses risk, and provides controls and tests to ensure compliance is maintained.
- However, assessments are suggested, not required.

Entity B
- 3 year work plan for 693 standards, including quarterly assessments.
- Assessments consider:
  - Risk to reliability
  - Prior non-compliance/corrective action
  - Identified lessons learned
  - Region’s compliance schedule
  - Requests by Standards’ Owners
  - Industry information
  - Entity uses industry experts and independent consulting firms for some assessments.
- No CIP monitoring program - under development.
Question 12

- How has the company responded to prior wrongdoing? Did it take disciplinary action against employees involved in violations? When misconduct occurs, is it a repeat of the same offense or misconduct of a different nature?

  • The ICP should include a direct tie from failure to follow Reliability Standards to disciplinary action, up to and including termination

  • Common deficiency - the ICP lacks direct mention of discipline
Question 12
How has the company responded to prior wrongdoings?

Entity A

- No discussion of prior non-compliance
- The Corporate Compliance Committee adopted a Disciplinary System Policy
  - an employee that has violated the corporate code of ethics or other rule may be subject to discipline, up to an including immediate dismissal and/or civil action.

Entity B

- No discussion of prior non-compliance
- Discipline addressed in Corporate Policy
  - Employees and contractors are accountable for performing job duties in compliant fashion
  - Willful violation will be dealt with pursuant to the “Disciplinary Guidelines Policy”
Does the company adopt and ensure enforcement of new and more effective internal controls and procedures to prevent a recurrence of misconduct?

- The ICP documentation should include a description of self assessment and should have enough steps or controls to keep the violation from occurring again
- Once weakness that it should be reported to top management (feedback loop) to work on how to strengthen the weakness
Question 13
How does the company prevent recurrence of non-compliance?

- Analyze, Solve, Prevent, Feedback Loop
  - Analyze via root cause analysis or some other method
  - Self Report if a compliance issue
  - Solve the problem
  - Determine how to prevent reoccurrence
  - Report back to Senior Management in a “feedback loop” to ensure ongoing review and enforcement and to ensure improvements in ICP Process (e.g. when, how new Standards are reviewed)
Question 13
How does the company prevent recurrence of non-compliance?

Entity A

- Plan to address future wrongdoings:
  - Entity has a procedure to address issues and aid in prevention of recurrence
  - assessment methodology is provided and assessment results are to be communicated to the cross-functional committee
  - policy to self-certify
  - The software tool would track the implementation of corrective actions

Entity B

- Plan to address future wrongdoings:
  - Through Mitigation Plans
  - Self-assessment procedure
Summary of Entity A’s ICP

Effective, but with some deficiencies. Potential areas of improvement or concern include:

- Program not cohesive or readily available to employees; not signed
- Independence not verified; Organizational structure and responsibilities not clear
- The entity’s policy does not promote Self-Reporting of possible violations
- ICP review stated as annually
- Training periods not identified
- No discussion of CIP vs. 693
- No discussion of response to prior non-compliance
- Minimal discussion on internal controls and prevention of future non-compliance
- A resource document was not provided (budget/personnel)
- The Compliance Policy does not require compliance actions
Summary of Entity B’s ICP

Effective, but with some deficiencies. Potential areas of improvement or concern include:

• Program not cohesive or readily available to employees; not signed
• Independence not verified; Organizational structure and responsibilities not clear
• The entity’s policy does not promote Self-Reporting of possible violations
• ICP review stated as annually
• Training periods not identified
• No CIP compliance monitoring program
• No discussion of response to prior non-compliance
• Minimal discussion on internal controls and prevention of future non-compliance
• A resource document was not provided (budget/personnel)
Include in ICP submittals

- Address 13 questions in detail
- Summaries and supporting documents, including:
  - Organizational chart (independence)
  - A hierarchy of program documents
  - Multiple documents cohesively build one program
- In-depth discussion on training
- Company’s viewpoint on self-reporting
- How often the company’s ICP is reviewed and updated
- Discuss CIP versus 693 compliance monitoring
- Company’s response to prior non-compliance
- Internal controls and how a future recurrence would be prevented
- Resource information (operating budget and personnel)

*Documents should be in alignment with each other*
First issued on March 18, 2010
- To add greater fairness, consistency, and transparency to its penalty determinations.

Suspended on April 15, 2010
- To afford entities the opportunity to submit written comments on them.

The Revised October 17, 2010 order stated:
- Penalty Guidelines will apply only to the Commission’s Part 1b investigations and enforcement actions.
- The Penalty Guidelines will not apply to the Commission’s review of NERC’s Notices of Penalty.
These seven factors are consistent with the four hallmarks and 13 questions

Unique is the emphasis on senior management for accountability and prior conduct

The order stated the Commission would likely give some degree of compliance credit to organizations that achieve these four factors, even if the organization failed to specifically meet each of the requirements explicitly listed in the Penalty Guidelines.
Questions?
Transparency of the Compliance Process

Jim Hughes
Manager of Registration and Certification
June 21, 2011, NERC Compliance Workshop
Topics of Discussion

- Transparency Initiatives
  - Lessons Learned
  - Alerts, CANs, CARs, Case Notes, RSAWs
  - Auditor Training and Useful Links

- Registration and Certification
  - Certification
  - Joint Registration Organization (JRO-Formerly Type I JRO)
  - Coordinated Functional Registration (CFR-Formerly Type II JRO)
The Lessons Learned documents are issued by the Events Analysis department and are designed to convey lessons learned from events.


June 7, 2011

- Two new lessons learned have been posted on the NERC Web site under the “Events Analysis – Lesson Learned” tab:

- The new lessons address the following topics:
  - RTU to SCADA Modem Path Vulnerabilities
  - Relay Protection and Coordination for Close-In Faults

- NERC welcomes any feedback on the information: [Earl.Shockley@nerc.net](mailto:Earl.Shockley@nerc.net)
Alerts

- Alerts are issued when NERC needs to put the industry or parts thereof on formal notice of potential or actual reliability concerns or issues.

- Three vehicles are used:
  - An advisory where no response action is required
  - A recommendation where recommendation for action is offered and responses tracked
  - Essential action where BOT-sanctioned actions are mandated

- They are available on the NERC website at http://www.nerc.com/page.php?cid=5|63
Case Notes

- Case Notes are examples of issues that the Regions are seeing in the field.
- The examples do not represent findings or recommendations but rather are an effort to disseminate information sooner rather than the NOP stage.
- Case Notes are updated every few weeks.
RSAWs

- Reliability Standards Audit Worksheets (RSAWs) are the ERO auditors’ worksheets by standard
- These worksheets are provided publically to provide transparency to the Registered Entities
- The RSAWs can be found at the NERC website here: http://www.nerc.com/page.php?cid=3\|22
Compliance Application Notices

Mike Moon
Director of Compliance Risk Management
June 21, 2011, NERC Compliance Workshop
FERC Order No. 693

- Commenters argued there were gaps and ambiguities in the standards and requested relief from monetary penalties and compliance.
- Paragraph 274 FERC opined:

  As discussed in our standard-by-standard review, each Reliability Standard that we approve contains Requirements that are sufficiently clear as to be enforceable and do not create due process concerns.
FERC Order No. 693

- Paragraph 277. The Commission agrees with NERC that, even if some clarification of a particular Reliability Standard would be desirable at the outset, making it mandatory allows the ERO and the Regional Entities to provide that clarification on a going-forward basis while still requiring compliance with Reliability Standards that have an important reliability goal.
Introduction and Basis for CANs

Therefore, CANs provide necessary compliance guidance as standards are revised and developed and fulfill our obligations per FERC Order No. 693

- Compliance guidance going forward and
- Responds to the industry’s request for compliance guidance and transparency.
Compliance Application Notices

**Purpose**
- To provide *transparency* to industry on how ERO auditors will apply compliance criteria to a Reliability Standard
- Establish *consistency* in the application of compliance criteria across all regions

**Process**
- Posted on website
- Evolving as process matures
- Responding to industry requests and comments
To submit a topic, email cancomments@nerc.net
Benefits of CANs:
- Consistency of compliance applications
- Transparency and Visibility into audit practices
- Timeliness – approximately 3 months to develop

CAN Development Status:
- Posted Final – 16
- FERC/Canadian Regulators – 6
- Posted for Industry comments – 4
- In Development – 19
- Identified Issues – 23 in queue
Options if you disagree with a CAN:

- Request Standard Interpretation
- Request Standards Authorization Request (SAR)
- Contest violation(s)
- Provide NERC with persuasive technical reasoning to change a CAN

NERC Compliance Operations welcomes your comments, questions and feedback about CANs at cancomments@nerc.net
Compliance Analysis Reports

Jim Hughes
Manager of Registration and Certification
June 21, 2011, NERC Compliance Workshop
Compliance Analysis Reports

- **Purpose:**
  - To provide transparency to industry on historical violation information
  - To provide in depth Regional violation analysis
  - Give recommendations to the industry on a Requirement basis for compliance

- **Process:**
  - NERC working to have Compliance Analysis Report process start to mirror the CAN process
  - NERC welcomes industry feedback for report topics
To submit a topic, email Ryan.Stewart@nerc.net
Compliance Analysis Reports

- Reports to date
  - PRC-005
  - CIP-004
  - FAC-008 & FAC-009
  - CIP-001
  - VAR-002
  - PER-002
  - CIP-006 & CIP-007
  - VAR-002 (and addendum)
  - EOP-005
  - TOP-002 (in development)
ERO Auditor Training

- Feb, 2011: ERO Auditor’s Workshop
  - 88% (100) auditors and managers
  - 693 and CIP
  - Addressed consistency issues
  - Next Workshop in September

- Completed 2 lead auditor training sessions
  - 2 more scheduled this year
Useful Links

- Compliance Application Notices (CANs)

- Compliance Analysis Reports (CARs)

- Case Notes

- Event Analysis Lessons Learned

- 2011 Actively Monitored List
Purpose and Background

Purpose: To provide an update on Registration and Certification processes, procedures, and responsibilities (Section 500 and Appendix 5A)

- Background - Industry Feedback
  - Need clarity regarding certification for BA, TOP, & RC
  - Need clarity regarding JRO registrations
  - Recent changes to the NERC Rules of Procedure Section 500 and Appendix 5A addressed these issues
Organization Certification – New Entity

- Scope is for BA, TOP, or RC only
- New entity must pre-certify before going operational
  - Entity must submit application to the region(s)
  - No compliance issues because the entity is not operating
  - Process takes 1-9 months to complete
  - Entity must go operational within 1 year after being certified
The Organization Registration & Certification Subcommittee (ORCS) established a process:

- Already operating BA, TOP, or RC;
- Has completed a compliance audit in the applicable function(s); and
- Has completed a readiness assessment in the applicable function(s)

If the entity has not completed the above, a certification review will be completed by the Regional Entity with NERC.
Organization Certification – Change/Expansion

- Entity is already certified as a BA, TOP, or RC
- Per RoP Appendix 5A, Items to consider when this entity may need to certify:
  - Changes to an entity’s footprint or operational challenges (i.e., TLRs) due to the changes
  - Organizational restructuring that could impact the BPS reliability
  - Relocation of the control center
  - Changes to entity ownership requiring major operating procedure changes
Organization Certification – Change/Expansion

- Significant changes to JRO / CFR assignments or agreements
- Complete replacement of a SCADA/EMS

The decision to certify this Entity is a collaborative decision between NERC and the Regional Entity

- It could be an aggregate of the above

NOTE: Focus will be on the changes.
Joint Registration Organization (JRO)

- Identified in RoP 507
  - Entity may register for itself and one or more of its members for one or more functions
  - Takes full compliance responsibility for itself and its member(s)
  - Application made to the Regional Entity(s)
  - The JRO must have an agreement with its member(s)
  - JROs posted on NERC Web (Formerly Type I JRO)
  - The JRO is responsible for all CMEP activities

- Typically a Co-Op, G&IT, or JAA
Coordinated Functional Registration (CFR)

- Identified in RoP 508
  - Entity may register with one or more entities for a single function
  - Divides compliance responsibility amongst themselves
  - Application made to the Regional Entity(s)
  - Application must identify the entity that is the Point Of Contact (POC)
  - Agreement clearly articulating and listing the division of responsibilities (typically a matrix)
  - List (matrix) must be kept up to date by the POC
Coordinated Functional Registration (CFR)

- CFRs posted on NERC Web (Formerly Type II JRO)
- CFR does not change compliance responsibilities for other function(s) that each entity in the CFR may be registered for
- Region is to ensure no unnecessary duplication or areas lacking in the CFR

- Any questions regarding Certification, Registration, JRO or CFR: Jim.Hughes@nerc.net
What to Expect in an Audit

Jim Hughes
Manager of Registration and Certification

June 21, 2011, NERC Compliance Workshop
Agenda

- Compliance Monitoring
- Continuous Preparation
- Perspectives on the Audit Program
- What is an Audit?
- The Audit and Spot Check
  - Planning
  - Conduct
  - Follow up
- Summary
Compliance Monitoring

Discovery Methods:
- Audit
- Spot Check
- Investigation
- Self Report*
- Data Submittals*
- Self Certification*
- Exception Reporting*
- Complaint

*Self identified violations
Continuous Preparation

- Use all self identified discovery methods.
- Develop internal controls for the Actively Monitored List and all other applicable standards.
- Develop a multi-year plan for continuous internal compliance monitoring.
- Identify your risk and performance profiles.
- Know/Implement your ICP.
Perspectives on the Audit Program

- Audit should be used as a tool to support higher levels of reliability.
- Need to leverage tech skills – and blend in auditing.
  - Use of SMEs, peers, CANs, CARs, Lessons Learned.
- RSAWs were a major improvement – but can be improved.
- There has been improvement in process and greater uniformity – but still more work to do.
Continued evolution needs to include:

- Use of ERO consistency and transparency tools.
- Breakthrough the fear and distrust of the compliance.
- Shift to performance based auditing; meet the goals of the program – e.g. increased reliability.
- Auditing is a tool to higher level of reliability.

Appropriate oversight of CMEP by FERC and NERC is essential.
An audit is an evaluation of a person, organization, system, process, project or product.

ERO Audit:

- Does not presume violation.
- Performed to ascertain the **validity** and **reliability** of information.
- Expresses an opinion or determination whether the entity meets a “standard” or does not meet a “standard” based upon a systematic review using an evidentiary review standard (“findings”).
- Seeks to provide **reasonable assurance** of the Registered Entities findings and non-findings.
Audits must provide Reasonable Assurance that evidence is sufficient and appropriate to support the auditors’ findings and conclusions.

- **Appropriate evidence**
  - Relevant to Reliability Standard requirements
  - Valid – has sound reasoning
  - Document Quality

- **Sufficient evidence**
  - Measure of quantity
  - “Weak” evidence, such as testimonials, need to be corroborated with more evidence
Audits are not just checking if things happened or if compliance requirements were met – they can be used to provide great value to the Registered Entity.

- Informal recommendations for process improvements or how to better demonstrate compliance are a natural by-product of an audit.

- Audits serve the public and industry interests.
  - There is a reliance on auditor’s work to identify risks.
  - It’s the responsibility of the Registered Entity to comply and take necessary action to meet standards.
CMEP is based to a large extent on the Generally Accepted Government Auditing Standards (GAGAS).

Three components:

- Plan the work – GAGAS Chapter 7
- Perform the work – GAGAS Chapter 7
- Report the work – GAGAS Chapter 8
Planning-Audit Notification

- Regional Entity will provide at least 90 days prior to the Compliance Audit.
  - Scope of the audit
    - Covers audited period
  - Appropriate RSAWs
    - Includes request for identification of SME for each applicable standard.
  - Timeline for providing evidence

- Prepare to demonstrate your organization’s “Culture of Compliance”.
Planning-Audit Preparation

- Understand applicable Reliability Standards which apply to your organizations’ registration.
  
  • **Best Practice:**
    
    - Embed the electronic evidence in the RSAWs supplied by the Regional Entity; or
    
    - Develop a folder for each applicable standard and place the standard and the evidence in the applicable folder.
  
  • Clearly identify appropriate sections in the electronic files used for evidence.
    
    - Reference the Reliability Standard and Requirements.
Audit Preparation (Continued)

- Program documents used as evidence need to include:
  - Approval signature(s) Required
  - Revision History
    - Include the last review date
  - Document Owner
    - Person responsible for maintaining document

- Prepare to substantiate Corporate Plans and Program documents with additional evidence.
Audit Evidence – Is it organized by Reliability Standard? Is it easily identified and located?

Examples of evidence could include:

- Database list
- EMS screen shots
- Maintenance and testing records
- Field Records
- Operator Logs
- Emails and US Mail
- Voice Recordings
Audit Conduct

A successful audit begins with:

- Registered Entity Executive Management involvement and support.
- A quality opening presentation by the Registered Entity.
- A quality opening presentation by the ERO audit team.
Registered Entity Opening Presentation:

- Corporate structure, including any affiliates
- High level overview of system
  - E.g. Statistics, Characteristics, Interconnections, neighboring entities, registration
- Scope of Entity’s Internal Compliance Program
  - Compliance performance history
- Delegated requirements (to and from)
  - Review Public Notice - NERC Compliance Process #2010-004 v1.0
- Scheduled Control Room and facilities tour
Audit Team Opening Presentation:
- Introduction of audit team
- Schedule
- Audit objective, methodology, and scope
  - Rationale for adjustment of scope
- Authorities and responsibilities
  - FERC Order 672 and 18CFR39
  - Roles and responsibilities of observers
- Confidentiality of information
- Audit timeline
- Sampling Methodology, if applicable
- Communications between entity and audit team
  - E.g. Data requests, Daily briefings, etc.
Registered Entity and ERO audit team should establish a daily routine:

- Start time and schedule for week.
- Objectives by day (to be adjusted each evening).
- SMEs are well prepared to present their evidence.
- End of day review and schedule adjustment.
  - Include status of all PVs
Audit Team Exit Presentation:

- Review
- Assessment of Compliance
  - Compliance Audit Summary
  - Findings, including PVs
- Due Process
- Post Audit Process & compliance Audit Report
  - Report process & timeline
- Noteworthy Observation
- Recommendations
- Performance Risk-Based Approach
Unusual Circumstances

- Irregularities such as falsified records, potential concealment, etc.
- Coordination with investigations or other open enforcement actions
- Dealing with difficult people and situations
- Dealing with impairments
  - Example: Role of observers and individual audit team members behavior
- Third party attestations (and work of others)
- Exercising judgment – escalating material risks for immediate corrective actions
Summary

- Preparation and management involvement are key
  - SMEs are well prepared
  - Dry run with critical compliance eyes with SME-mock audit/invite peers

- Know and implement your ICP
- Review CANS, CARS, Bulletins, etc
- End of day debriefs are very important
Questions?
Overview

- Reliability / Compliance Excellence
- ERO Event Analysis Process
  - Purpose, Philosophy, and Background
- Event Analysis Field Trial Status
  - Events / Category / Region
  - Types of events / trends
  - Lessons learned development
  - Revisions to Process Document
- Next steps
Reliability Excellence

Lab Tests Confirm Salmonella Source
Reliability/Compliance Excellence

Reliability Excellence
- Best practices, benchmarking
- Engrained behaviors
- Compliance margin
- Continuous improvement

Compliance Excellence
- Senior management engagement
- Preventive measures
- Detection, cessation, reporting
- Remediation
Purpose of New EA Program

To ensure the reliability of the North American bulk power system

- **Analyze and understand system events**
  - Individual Events
  - Periodic review of events in aggregate to detect emerging trends and signs of decline in reliability performance

- **Determine Actual and Potential Risk**
  - Categories are used to denote actual and potential risk of events and to guide associated actions
  - Response is different based on category

- **Promote ERO Enterprise as a Learning Organization**
  - Publishing of Lessons Learned/Alerts in a timely manner

- **Includes appropriate Compliance Review**
Event Analysis – Goals & Philosophy

- **Goal 1:** Promoting BPS Reliability
- **Goal 2:** Behavior / Cultural
  - Enhance / Refine “Reliability Excellence”
  - Collaboration (ERO-wide)
  - Promote “Learning Organization”
- **Philosophy:** Event significance / risk varies
  - Actual / Potential
  - Response reflects significance / other circumstances
EA Program Philosophy

- Prioritize the analysis process (risk & significance)
- Promote timely systematic reporting
- Predictable and proportional actions
- Promote Excellence Cultures (reliability/compliance)
  - “Learning Organization”
  - Critical Self Evaluation
  - Sharing of Lessons Learned
  - Timely Self Reporting
Event Categorization

Prioritizes Event Analysis based on risk and significance, response is systematic and the depth of analysis increases as the category rises.

Cat 1
Unintended loss of bulk power elements (Gen, transmission components, intended or controlled separations)

Cat 2/3
Loss of a generation stations, loss of small to medium amounts of load, Unintended system separations and islanding

Cat 4/5
Loss of large amounts of load or generation. Large Unintended large system separations and Islanding

Response
Event Analysis — Key Steps

- What Happened
- Why It Happened
- Lessons Learned
- Gap Analysis
- Corrective Actions
- **Trend Analysis/Themes?**

Systematic analysis based on Industry Standard Cause Analysis methods
**Initial Notification**
- By Registered Entity
- Within 24 Hours
- Sent to Region & NERC

**Brief Report**
- By registered entity
- Sent to Region & NERC
- Items identified in Appendix “A”

**Lessons Learned**
- Entity, Regional Development
- Sent to EAWG for Review
- NERC, and
  - Tracks
  - Reviews
  - Publishes on NERC web Page

**Event Analysis Report (EAR)**
- By Registered Entity
- Detailed Sequence of Events
- Actual system response
- Causal Analysis Methodology
- Causal Factors/Contributors
- Root Cause
- Corrective Actions
- Industry Recommendation
- Sent to Region and NERC
## EA Process – Target Reporting Timelines

<table>
<thead>
<tr>
<th>Event Category</th>
<th>Brief Report</th>
<th>Draft Lessons Learned</th>
<th>EAR</th>
<th>Compliance self-assessment</th>
<th>Close Event Analysis</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Draft within 5 business days, sent to applicable Regional Entity for review. Final report within 10 days.</td>
<td>Within 15 business days</td>
<td>Not required</td>
<td>Encouraged (submittal not required)</td>
<td>10 business days following receipt of Brief Report</td>
</tr>
<tr>
<td>2</td>
<td>Draft within 5 business days, sent to applicable Regional Entity for review. Final report within 10 days.</td>
<td>Within 30 business days</td>
<td>30 business days</td>
<td>Initial (list of standards/requirements being reviewed) within 20 business days Final within 60 business days after Brief Report</td>
<td>30 business days following receipt of EAR</td>
</tr>
<tr>
<td>3</td>
<td>Draft within 5 business days, sent to applicable Regional Entity for review. Final report within 10 days.</td>
<td>Within 30 business days</td>
<td>60 business days</td>
<td>Initial (list of standards/requirements being reviewed) within 20 business days Within 90 business days after Brief Report</td>
<td>30 business days following receipt of EAR</td>
</tr>
<tr>
<td>4</td>
<td>Draft within 5 business days, sent to applicable Regional Entity for review. Final report within 10 days.</td>
<td>Within 60 business days</td>
<td>120 business days</td>
<td>Initial (list of standards/requirements being reviewed) within 20 business days Within 150 business days after Brief Report</td>
<td>60 business days following receipt of EAR</td>
</tr>
<tr>
<td>5</td>
<td>Draft within 5 business days, sent to applicable Regional Entity for review. Final report within 10 days.</td>
<td>Within 60 business days</td>
<td>120 business days</td>
<td>Initial (list of standards/requirements being reviewed) within 20 business days Within 150 business days after Brief Report</td>
<td>60 business days following receipt of EAR</td>
</tr>
</tbody>
</table>
Lessons Learned Preparation and Processing

- Registered Entity & Region work together to prepare lesson using the template in Appendix D
- Registered Entity & Region sanitize the lesson to remove all indication of the entity involved in the event and any other event details which are confidential
- Region will post to secure FTP site
- Region will notify NERC staff that the Lesson has been posted
- NERC staff will review lesson
- NERC staff will add lesson to Master List, prioritize lessons and identify common themes
- NERC staff will distribute to EAWG for review and discussion
- Region that submitted the lesson or NERC will lead EAWG discussion/review
- Region or NERC will make improvements based on EAWG input
- Region will send lesson to the involved registered entity for review, if needed based on changes made
- NERC will post on Website and send notification email to industry
Compliance Self Assessment (Entity)

- Encourage entities - establish compliance liaison
- List implicated Standards/Requirements
- Written analysis/disposition
- IRAC (type) systematic method
  - Issue
  - Rules
  - Analysis
  - Conclusion
- Conservatively self-report possible violations
Events Analysis – Benefits / Challenges

- Consistency, Predictability, Transparency
- Lessons Learned
  - Event specific
  - Cross-cutting
- Differentiation
  - Significance / risk
  - Behaviors / culture
- Paradigms
- Reporting
  - Timely
  - Comprehensive
- Communications
- Systematic Compliance Assessment
Event Analysis Field Trial Status
321 occurrences Recorded Between Oct 25 2010 and April 25, 2011

128 events qualified for review under the field trial (Cat 1 - 5)
Events/Category/Region

Events 10/25/10 - 5/25/2011

A | B | C | D | E | F | G | H

Cat 5 | Cat 4 | Cat 3 | Cat 2 | Cat 1 | Cat 0
Event Analysis Report (EAR) Submittals

51 EAR's Submitted During the Field Trial

<table>
<thead>
<tr>
<th>Region</th>
<th>EAR's Submitted</th>
</tr>
</thead>
<tbody>
<tr>
<td>A</td>
<td>4</td>
</tr>
<tr>
<td>B</td>
<td>5</td>
</tr>
<tr>
<td>C</td>
<td>7</td>
</tr>
<tr>
<td>D</td>
<td>2</td>
</tr>
<tr>
<td>E</td>
<td>6</td>
</tr>
<tr>
<td>F</td>
<td>2</td>
</tr>
<tr>
<td>G</td>
<td>15</td>
</tr>
<tr>
<td>H</td>
<td>10</td>
</tr>
</tbody>
</table>
Candidate Lessons Learned (by Region)

51 Candidate Lessons Learned from 128 “Qualifying” Events (10/25/10-5/25/11)

Lessons Learned by Region

<table>
<thead>
<tr>
<th>Region</th>
<th>Lessons Learned</th>
</tr>
</thead>
<tbody>
<tr>
<td>A</td>
<td>4</td>
</tr>
<tr>
<td>B</td>
<td>4</td>
</tr>
<tr>
<td>C</td>
<td>6</td>
</tr>
<tr>
<td>D</td>
<td>5</td>
</tr>
<tr>
<td>E</td>
<td>3</td>
</tr>
<tr>
<td>F</td>
<td>5</td>
</tr>
<tr>
<td>G</td>
<td>6</td>
</tr>
<tr>
<td>H</td>
<td>18</td>
</tr>
</tbody>
</table>
Lessons Learned - Themes

Cross Cutting Lessons Learned
51 Lessons Learned Submitted since Start of the Field Trial
Oct 25, 2010 - May 25, 2011

- Generators 22%
- Facilities Design, Connections, and Maintenance 24%
- Communications 15%
- Personnel Performance, Training, and Qualifications 7%
- Resource and Demand Balancing 9%
- Testing/Commissioning 16%
- Other 32%
- plans and procedures 7%

NERC
North American Electric Reliability Corporation
128 Qualified Events between Oct 25, 2010 and April 25, 2011

A                        B                        C                        D                       E

F                        G                       H

Appendix G / Entity Compliance Assessment

Appendix G
Self-reports
February 4 – 6, 2011 Sunbelt Cold Snap Event
What’s New: Field Trial Phase 2 Summary

- Incorporate an Event Notification (within 24 hrs of qualifying event)
  - The event report form is being recomposed to capture key data required in the initial event notification
  - The event notification will be made to NERC Situational Awareness (set up email box) and the applicable region(s) in parallel

- Institute Data Hold for Category 2 and above

- Update to Event Reporting and Analysis Timeline
  - The remaining section of Event Report form (beyond the event notification) will be completed within 10 business days of the event notification.

- Registered Entities will complete an Event Analysis Report and a compliance self evaluation for Cat 2 and above

- Registered Entities will be strongly encouraged to complete a compliance evaluation for all qualifying events (Cat 1 and above)
What’s Next – Field Trial Phase 2

- Phase 2 started on May 5, 2011 (version 2 process)
- Check and Adjust in July 2011
- NERC Rules of Procedure in Nov 2011
Enforcement Violation Processing: Keeping Industry, Regional Entities, and NERC Accountable

Rebecca Michael, Associate General Counsel
Ed Kichline, Manager of Enforcement Processing

June 21, 2011, NERC Compliance Workshop
Agenda

- ERO Process
- FERC Process
- Risk and the Entity’s Story
- Reconciliation and Resolution
- Finalization
- Summary
Regional Entities are responsible for the intake of most violations and process them with Registered Entities through a settlement agreement or confirmation of a violation.

- Notices sent by the Regional Entity describe the options of the Registered Entity for responding to the notices and commencing settlement.
- Registered Entities should engage with the Regional Entity early and often, making intentions as clear as possible.
- Registered Entities should be familiar with the due process mechanisms included in the NERC Rules of Procedure, including Appendix 4C which contains the Compliance Monitoring and Enforcement Program (CMEP).
How Violations Get to NERC (cont’d)

- Violations sent in a Settlement Agreement between the Registered Entity and the Regional Entity
  - The Agreement, including the penalty, is the result of negotiations between the parties
- Violations sent in a Notice of Confirmed Violation prepared by the Regional Entity
A Notice of Confirmed Violation (NOCV) is issued to a Registered Entity confirming a violation of one or more Reliability Standards, as a result of

- (1) the Registered Entity accepting, not contesting or not responding within 30 days to a Notice of Alleged Violation and the proposed penalty or sanction, or
- (2) the finding of a violation through a hearing and appeal, or
- (3) the expiration of the period for requesting a hearing or an appeal, or
- (4) the Registered Entity admitting the violation as part of an executed settlement agreement.
Settlement Agreements

- The vast majority of violations come to NERC in Settlement Agreements

- An NOCV may offer swifter resolution of possible violations
NERC evaluates the record provided by the Regional Entity to:

- Verify the violated Standard applies to the facts and circumstances
- Evaluate the risk assessment
- Apply NERC’s Sanction Guidelines to determine if the penalty bears a reasonable relation to the seriousness of the violation and the remedial actions of the registered entity
- Promote consistent outcomes across the Regional Entities for violations of similar standards involving similar registered entities

NERC sends approved Settlement Agreements and NOCVs to FERC for review through the filing by NERC of Notices of Penalty (NOPs)
The NOP process is only one part of the larger picture in terms of compliance, but it serves important functions:

- NOPs set forth the ultimate disposition of a violation
- NOPs provide information that allows other entities to identify similar issues or to avoid them
How NERC Sends Violations to FERC

- **FERC Guidance on NOPs**
  - *Statement of Administrative Policy on Processing Reliability Notices of Penalty and Order Revising Statement in Order No. 672, 123 FERC ¶ 61,046 (2008)*
  - *Further Guidance Order on Filing of Reliability Notices of Penalty, 129 FERC ¶ 61,069 (2009)*
  - *Order Initiating Review of Notice of Penalty, 130 FERC ¶ 61,151 (2010)*
  - *Notice of No Further Review and Guidance Order, 132 FERC ¶ 61,182 (2010)*
  - *Order on Review of Notice of Penalty, 134 FERC ¶ 61,209 (2011) reh’g pending (Turlock Order)*
How NERC Sends Violations to FERC

- NOPs generally contain:
  - Basis for determination
  - Source document
  - Disposition of violation, including registration, violation, discovery, and mitigation information
  - Mitigation plan
  - Certification of completion of mitigation plan
  - Verification of mitigation plan
How NERC Sends Violations to FERC

**NOP Formats**

- Abbreviated Notices of Penalty for violations that did not pose a serious or substantial risk to reliability
- Full Notices of Penalty for violations that posed a serious or substantial risk to reliability
- Administrative Citation Process (ACP)
ACP NOPs include:

- Violations that do not pose a serious or substantial risk to reliability
  - Violations that are fully-mitigated
  - Violations that are not indicative of a pattern of violations

- Each violation treated as a single line item on a spreadsheet
  - Basic Identification (Entity Name, Region, NCR_ID, Violation ID)
  - Violation Description
  - Standard, VRF, VSL, Discovery Method, Penalty
  - Risk Assessment
  - Mitigation

- Regional Entities maintain supporting documents, including brief Settlement Agreement
To date, NERC has filed 472 Notices of Penalty, which represent over 2,200 violations with penalties ranging from $0 to $450,000

- FERC has affirmed or let stand 454 Notices of Penalty that NERC has filed, which includes two Omnibus filings and five ACP filings
  - Rehearing remains pending in two dockets
- Another 18 NOPs (the difference between 472 and 454 NOPs) are awaiting Commission action expected in June
FERC Review of NOPs

FPA section 215(e)(2) provides that a penalty NERC or a Regional Entity imposes may take effect no earlier than 31 days after NERC files with the Commission a notice of penalty and the record of proceedings.

FPA section 215(e)(2) further states, “Such penalty shall be subject to review by the Commission, on its own motion or upon application by the user, owner or operator that is the subject of the penalty filed within 30 days after the date such notice is filed with the Commission.”
How NERC Sends Violations to FERC

- **NOP Processing Timeframes (18 C.F.R. § 39.7(e)(1))**
  - Entity subject to an NOP may file an application for review of it within 30 days of the date NERC files the NOP.
    - Any answer, intervention or comment to an application for review of a proposed penalty must be filed within 20 days after the application is filed, unless otherwise ordered by the Commission.
    - If the entity subject to a proposed penalty files an application for review of the proposed penalty, the Commission will take action on that application within 60 days of the date on which it is filed, unless the Commission determines on a case-by-case basis that an alternative expedited procedure is appropriate.
How NERC Sends Violations to FERC

- NOP is also subject to review by the Commission on its own motion within 30 days after the date of the filing.
  - In such a case, FERC would generally allow interventions within a 20 day period and a FERC decision could be expected within 60 days. These timeframes, however, are not mandated in the regulations.
  - FERC also may take action within 30 days of the filing of an NOP to prevent a proposed penalty from being affirmed by operation of law on the expiration of that 30-day period.
Scope of FERC Review of NOPs

The review may involve the proposed penalty or its type (i.e., monetary penalty vs. non-monetary penalty, for example) as well as of any determinations underlying the proposed penalty, including whether a violation of a Commission-approved Reliability Standard occurred or whether there is a sufficient factual record to support any such determination.

FERC reviews the record *de novo*, to determine that it supports the proposed penalty.
Assessing actual impact of a violation, as well as its potential risk
- The vast majority of violations have resulted in no actual harm to the reliability of the bulk power system
- Main task is to determine the potential risk of the violation
- Not enough to say that nothing bad happened

Conducting a “Yes, but…” analysis
- Yes, there was a violation, but the risk was reduced because of:
  - Compensating measures put in place by the registered entity
  - Compensating factors outside of the registered entity’s control
  - Operating characteristics of a particular facility
  - Limited scope of the violation
Examples of Helpful Risk Considerations

- Yes, we violated PRC-005-1 R2, but…
  - We had monitoring devices with alarms on our Protection System devices
    - And we had no alarms activated during the violation period

- Yes, we violated CIP-004-3 R3, but…
  - We only missed one Personnel Risk Assessment (PRA) out of hundreds
  - The violation involved long-standing employees with no negative work history
Telling the Registered Entity’s Story

- Start at the beginning
  - Self-Report
  - Self-Certification
  - Audit Report
  - Spot Check
  - Other discovery methods

- Get the facts out there as quickly, and accurately, as possible

- Engage with the Regional Entity on framing the Settlement Agreement or the NOCV
How to Have a Better Story

- Find the problem on your own
  - Do not wait until a pending self-certification to perform internal audits
- Fix the problem when you find it
- Report the problem as soon as you can
  - Possible violations do not need to be mitigated before a Self-Report
- Submit a Mitigation Plan as soon as you can
  - Displaying effective and timely remediation vs. Only following the requirements of the CMEP
  - Submitting a Mitigation Plan is not admitting a violation
  - Work with your Regional Entity
Resolving the Story: The Mitigation Plan

- Describe how you fixed the problem
- Describe how you are preventing the problem from recurring
  - Specific actions and milestones
  - “Above and beyond” activities
- Describe the cause of the problem and how the actions in your plan address the problem and promote reliability
  - Area of emphasis for NERC going forward

Show your accountability by timely recognizing the problem and implementing the solution
Resources for Mitigation Plan Information

- Case Notes are based on information in mitigation plans that have been accepted by Regional Entities and approved by NERC
  - These are posted in advance of the conclusion of an enforcement action as applicable
  - NERC believes that the actions Registered Entities are taking may be useful to others to identify and avoid similar issues.
  - NERC is not posting summaries of all mitigation plans. Rather, the focus is on novel issues, high quality mitigation plans, detailed responses as to actions taken, or to address relevant issues seen in the field.
Case Notes identify: Reliability Standard, Requirement, Risk and Mitigation Action Taken

NERC does not identify the Regional Entity, region, location or any identifying information

As of June 21, 2011, 70 Case Note examples have been posted

The goal is to publish 4 or 5 Case Notes every couple of weeks
Resolving the Story: The Mitigation Plan

Case Notes can be found under Resources on the Compliance page of our website.

Or you can follow the following link: http://www.nerc.com/page.php?cid=3|22|371
Resolving the Story: The Mitigation Plan

<table>
<thead>
<tr>
<th>RELIABILITY STANDARD</th>
<th>REQUIREMENT</th>
<th>FACTS</th>
<th>RISK</th>
<th>MITIGATION ACTION TAKEN</th>
</tr>
</thead>
<tbody>
<tr>
<td>CIP-001-1</td>
<td>1</td>
<td>The entity lacked procedures for the recognition of and for making operating personnel aware of sabotage events on its facilities and multi-site sabotage affecting larger portions of the Interconnection.</td>
<td>Personnel may not have been prepared for potential sabotage events.</td>
<td>The entity updated its procedures for sabotage recognition. In addition, the entity's System Operations Trainer put together a PowerPoint presentation containing this information, and presented it to the System Operators. The Sabotage Awareness PowerPoint Presentation was posted as a streaming video on the internal employee training site. A section was added to the Entity's Employee Handbook outlining Sabotage Recognition and Reporting. Additionally, an internal article was published outlining the need for Sabotage Recognition and Reporting and making employees aware of the changes to the handbook as well as the availability of the PowerPoint training materials on the internal site.</td>
</tr>
</tbody>
</table>
## Resolving the Story: The Mitigation Plan (cont’d)

<table>
<thead>
<tr>
<th>RELIABILITY STANDARD</th>
<th>REQ.</th>
<th>FACTS</th>
<th>RISK</th>
<th>MITIGATION ACTION TAKEN</th>
</tr>
</thead>
<tbody>
<tr>
<td>CIP-002-1</td>
<td>R3.1</td>
<td>The entity failed to identify certain workstations as Critical Cyber Assets.</td>
<td>Without proper identification, a Critical Cyber Asset may not receive the appropriate levels of protection.</td>
<td>The entity 1) removed remote access to the energy management system (EMS) control functions from workstations not defined as Critical Cyber Assets; 2) established Physical Security Perimeters and Electronic Security Perimeters for all locations where monitoring and control function of the EMS is allowed; and 3) identified the workstations as Critical Cyber Assets.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>CIP-004-3</td>
<td>R3.2</td>
<td>The entity was calculating the interval for completing seven-year personal risk assessments (PRAs) based on an individual’s hire date, rather than the date of his/her last PRA.</td>
<td>Using an individual’s hire date does not ensure the individual is current with his/her PRA.</td>
<td>The entity 1) completed all necessary seven-year PRAs; 2) completed a review of all individuals with a PRA report; 3) updated its personnel tracking system to reflect last date of PRA as opposed to hire date; 4) updated its documentation to reflect process improvements; 5) completed a reconciliation to determine that all personnel (including contractors) are in the personnel tracking system; 6) developed and administered training; and 7) utilized an outside consultant to perform an independent review of its processes.</td>
</tr>
</tbody>
</table>
## Resolving the Story: The Mitigation Plan (cont’d)

<table>
<thead>
<tr>
<th>RELIABILITY STANDARD</th>
<th>REQ.</th>
<th>FACTS</th>
<th>RISK</th>
<th>MITIGATION ACTION TAKEN</th>
</tr>
</thead>
<tbody>
<tr>
<td>CIP-006-3</td>
<td>R2.2</td>
<td>The entity did not have the protective measures specified in the standard for Cyber Assets because it failed to identify certain devices as access control and monitoring devices.</td>
<td>Without proper identification, an access control and monitoring device may not receive the appropriate levels of protection.</td>
<td>The entity 1) conducted interviews with its network engineer to establish a course of action to implement the mitigation plan; 2) applied all required security protections; 3) updated all relevant documentation; and 4) communicated all updates to relevant staff.</td>
</tr>
<tr>
<td>CIP-007-3</td>
<td>R5</td>
<td>The entity had certain servers and workstations that utilized default accounts that could not be renamed, removed, or disabled. R5.2: In addition, passwords could not be changed and accessed shared accounts that require implementing a management use policy.</td>
<td>The inability to change, remove, or disable account names and password could weaken security, therefore increasing the risk of an unauthorized individual gaining access to sensitive information.</td>
<td>The entity 1) created a document with a plan to upgrade software in order to meet NERC compliance requirements for default accounts and passwords; 2) signed an agreement with a vendor for the upgrade on the system; 3) validated the functionality of the upgraded software in a non-production environment; 4) upgraded the software during a scheduled outage; and 5) validated the functionality of the upgraded software in a production environment.</td>
</tr>
<tr>
<td>RELIABILITY STANDARD</td>
<td>REQUIREMENT</td>
<td>FACTS</td>
<td>RISK</td>
<td>MITIGATION ACTION TAKEN</td>
</tr>
<tr>
<td>----------------------</td>
<td>-------------</td>
<td>-------</td>
<td>------</td>
<td>-------------------------</td>
</tr>
<tr>
<td>IRO-001-1</td>
<td>R8</td>
<td>Registered Generator Operator failed to comply with clear and concise electronic instructions and subsequent verbal instructions from the Reliability Coordinator to reduce and limit plant generation to keep the Special Protection System (SPS) from activating. The entity failed to reduce generation and the SPS activated, causing the plant to trip offline.</td>
<td>The SPS activation caused the plant to trip offline completely, causing generation to quickly reduce below the desired generation level. If the SPS had not correctly activated, generation would not have been reduced and the transmission line may have been overloaded.</td>
<td>This entity had appropriate procedures in place to follow directives by the Reliability Coordinator, so mitigation included personnel training. The entity provided additional training to its operators regarding procedures to be followed when it receives electronic or verbal instructions from the Reliability Coordinator, including transmitting the instructions to the generation facility personnel.</td>
</tr>
</tbody>
</table>
Resolving the Story: The Mitigation Plan (cont’d)

<table>
<thead>
<tr>
<th>RELIABILITY STANDARD</th>
<th>REQ.</th>
<th>FACTS</th>
<th>RISK</th>
<th>MITIGATION ACTION TAKEN</th>
</tr>
</thead>
<tbody>
<tr>
<td>BAL-002</td>
<td>R4</td>
<td>After a disturbance involving generation totaling 1,400 MW, the entity did not recover its Area Control Error within 15 minutes.</td>
<td>Not recovering the Area Control Error within 15 minutes may have required that the entity carry additional reserves.</td>
<td>1. The entity increased the system-wide Ten-Minute Reserve (“reserve bias” by 10%) to 110% of the first contingency loss. 2. The entity increased the minimum Ten-Minute Spinning Reserve requirement from 25% to 50% of the first contingency. 3. The entity required the Control Room system operators to maintain a mix of Shared Activation of Reserves (assistance from external Balancing Authorities) and other reserves, assuming a non-performance factor (the amount of reserves called on in addition to the source loss assuming less than 100% performance of requested resources) of at least 140% of first contingency loss. 4. The entity assessed the performance of generation resources during the event (potential changes to operating practices). 5. The entity modified the key software display by providing the Control Room System Operator with additional tools to view which Market Participant Generation units have not acknowledged electronic dispatch signals. 6. The entity modified internal system operating procedures by making clear that security-constrained economic dispatch solution should not be executed during an Area Control Error recovery period. 7. The entity conducted operator training. The entity included the procedure changes discussed above in training modules. A PowerPoint presentation was posted as a streaming video on the internal employee training site.</td>
</tr>
</tbody>
</table>
“Roll-up” Violations

- Violations of different Reliability Standards “related to a single act or common incidence of non-compliance” are generally assessed “a single aggregate penalty” consistent with Section 3.10 of the NERC Sanction Guidelines. The penalty, sanction, or remedial action will not be that determined individually for the least serious of the violations; it will generally be at least as large or expansive as what would be called for individually for the most serious of the violations.

- Violation of sub-requirements of a Reliability Standard may be treated as a single violation. NERC assigns a violation severity level only to each main requirement of a Reliability Standard. Thus, a violation of any number of sub-requirements would trigger only a single violation of the main requirement. This proposed methodology, referred to as “roll-up” methodology was approved by the Commission in *North American Electric Reliability Corporation*, 135 FERC ¶ 61,166 (2011).
NERC’s Treatment of the Story

- Multiple instances of violation of a single Standard
  - Example: failure to notify Transmission Operator of change in status of voltage control device under VAR-002-1.1b R3 = 1 Violation with several instances.
  - However, NERC or the Regional Entity is not constrained to assessing the same penalty amount for each of the multiple violations, irrespective of their proximity in time (Section 3.21 of Sanction Guidelines).
NERC’s Treatment of the Story (cont’d)

- Violation History of the Registered Entity and its Affiliates
  - Prior violations of same or similar standards involving similar conduct by the Registered Entity
  - Prior violations of same or similar standards involving similar conduct by affiliates of the Registered Entity where there is a commonality of compliance responsibility among the affiliates

A large number of violations does not have to be a negative factor, but there is a responsibility to learn from prior violations
Learning from Others’ Stories

- Notices of Penalty posted on NERC’s website under Compliance-Enforcement & Mitigation
  - Settlement Agreements, Self-Reports, and Mitigation Plans for non-CIP violations

- Case Notes for CIP violations
  - Description of nature of violation and mitigating activities
Reporting on dismissals is under development

- 27% of self-reports result in dismissals
- Providing details on dismissals could help Registered Entities incorporate risk-based monitoring into their own compliance programs
  - Focus the resources of Registered Entities
  - Ongoing, thorough and rigorous self-evaluation by Registered Entities to demonstrate effective internal controls that produce a comprehensive culture of self-reporting
NERC and the Regional Entities are committed to transparency and helping Registered Entities ensure reliability effectively and efficiently.
Registered Entities can help themselves throughout this process:

- self-report
- tell your own story clearly with detail
- work with the Regional Entity to develop an effective mitigation plan
- use the resources the ERO is providing
Contact Information

Mike Moon, Director of Compliance Operations
michael.moon@nerc.net, 404-446-2567

Val Agnew, Manager of Compliance Interface and Outreach
valerie.agnew@nerc.net, 404-446-2566

Jim Hughes, Manager of Organization Registration and Certification
jim.hughes@nerc.net, 404-446-2574

Earl Shockley, Director of Events Analysis and Investigations
earl.shockley@nerc.net, 404-446-2570

Rebecca Michael, Associate General Counsel
rebecca.michael@nerc.net, 202-383-2625

Ed Kichline, Manager of Enforcement Processing
edwin.kichline@nerc.net, 202-400-3025

cancomments@nerc.net