NPCC Compliance Monitoring Team
Classroom Session

Jenifer Farrell – Director, Compliance Monitoring
Jacqueline Jimenez – Manager, Compliance
Michael Stuetzle – Senior CIP Analyst
Cecil Elie – Senior CIP Analyst
Agenda

- 2020 CIP Self-Certifications
- 2019 Self-Certification Update
- Compliance Oversight Plans (COP)
- PRC-005 Data Requests (DR)
- Standards Update
- CIP Root Cause Analysis
- Open Forum for Questions
2020 CIP Self-Certifications

• The 2020 Compliance Monitoring schedule is posted on the [NPCC website](#).
• CIP Self-certification with evidence submittal
  – CIP-002-5.1a, R1 and R2
  – CIP-003-8, R2, Attachment 1 Sections 2, 3, and 5
• Self-certification notifications will be sent approximately in Q2 2020.
2020 CIP Self-Certifications

• Registered Entities will have 45 days to respond.

• NPCC will do a random selection of the entity submittals to choose the evidence to review.
  – Based on NERC Random Sampling Methodology
2019 Self-Certification Update

• **CIP-002-5.1a**
  - Requirements: R1, R2
  - Entities: 22
    • No Finding: 20
    • Not Applicable: 1
    • Potential Non-Compliance: 1
Compliance Oversight Plans (COP)

• Updated COP template approved in June 2019.
  – There are now 6 Oversight Strategy Categories.
  – All NPCC Registered Entities have been bucketed into a Category and assigned a Monitoring Interval.
  – Entities on the 2020 schedule will get a COP.
PRC-005 Data Requests (DR)

• PRC-005 pre-audit data request are included in the Audit Notification Package.
• Helps facilitate evidence review.
• Due 30 days after audit notification.
• Asks to provide a list of the protection equipment covered under PRC-005.
  – Must be in Excel format
PRC-005 Data Requests (DR)

- Ensure the spreadsheet contains:
  - Equipment ID
  - Last/previous test date
  - Current test date
  - Next/future scheduled test date
  - Battery type (NICAD, VRLA, VLA)

- Auditors will assign an NPCC data request ID and highlight the components for which they will review the detailed testing/maintenance records.
Organization of PRC-005 DRs

- When submitting the evidence for the sample set of components:
  - Create folders named with each **NPCC data request ID**.
  - Only place the maintenance records for the associated NPCC data request ID in folder.
  - Ensure the maintenance records are highlighted and/or annotated.
  - If document includes many pages, specify the page number in the document that supports compliance.
Examples

• Annotated evidence

  – **Good:**

  • The section is highlighted with a word bubble of the requirement it is satisfying.

### 4.3. Tested Contingencies

**Table 3 Voltage Contingency Definitions** lists the contingencies that were evaluated for each configuration studied.

<table>
<thead>
<tr>
<th>Contingency</th>
<th>ID</th>
<th>Elements lost</th>
<th>Line IDs</th>
<th>Voltage (kV)</th>
</tr>
</thead>
</table>

FAC-014-2 R1
The Reliability Coordinator shall ensure that SOLs, including Interconnection Reliability Operating Limits (IROLs), for its Reliability Coordinator Area are established and that the SOLs (including Interconnection Reliability Operating Limits) are consistent with its SOL Methodology.
Examples

• Annotated evidence
  – Poor:
    • Providing a document with no highlighting to identify the section to be reviewed or references to the exact page.
    • This can result in the auditors asking follow-up questions.
Examples

• PRC-005 submittal
  – **Good:**
    • Relay test records where all pertinent information is highlighted, i.e., Relay name, test date, type of test, test result (Pass/Fail)
    • Spreadsheet containing data by substation, that provided explanation of the spreadsheet and very clear column headings, i.e. component, description, manufacturer/model, operates/trips, test dates (last, current, future)
Examples

- **Poor:**
  - Relay test record with 313 pages of evidence. No pertinent information highlighted or annotated.
  - Spreadsheet with no column headings or test dates provided.
Standards Update

Cecil Elie
Senior CIP Analyst
CIP / O&P Standards Updates

- PRC-026-1 – 1/1/2020
- TPL-007-3 – 1/1/2020
- CIP-003-7 – 1/1/2020
- CIP-003-8 – 4/1/2020
- CIP-005-6 – 7/1/2020
- CIP-010-3 – 7/1/2020
- CIP-013-1 – 7/1/2020 (new standard)
- CIP-008-6 – 1/1/2021 (future reminder)
PRC-026-1 (R2-R4)
Effective Date of Standard 1/1/2020

• Relay Performance During Stable Power Swings

  R1 is already in effect (as of January 1, 2018)
  R2, R3, and R4 go into effect January 1, 2020

  This standard looks at relay performance during stable power swings.
TLPL-007-3 (R5 & R9)
Effective Date of Standard 1/1/2020

- Transmission System Planned Performance for Geomagnetic Disturbance Events

- R5 and R9 requires applicable entities to provide GIC Flow information specified in R6 and R10 to the TO and GO.
- The sub-requirements are inclusions to what the information needs.

- Read R5, R6, R9, R10 and Attachment 1
- Prepare your entity to submit information to your TO and GO.
CIP-003-7
Effective Date of Standard 1/1/2020

- **Cyber Security — Security Management Controls**

Review and approval from CIP Senior Manager every 15 calendar months on cyber security policies for:
  - High & Medium BES Cyber Systems
  - Low impact BES Cyber Systems from CIP-002

Implement documented cybersecurity plans for Low Impact BES Cyber Systems

Identify CIP senior manager by name and document changes within 30 days

Implement documented process to delegate authority
CIP-003-8
Effective Date of Standard 4/1/2020

- Cyber Security — Security Management Controls

This standard is almost identical to CIP-003-7 except for:
- Attachment 1 Section 5.2.2
- TCA’s handled by third party vendors for low impact BCS

Additional mitigation prior to vendor connecting TCA’s
CIP-003-(7,8)
Cyber Security — Security Management Controls
Requirements & Measures

**High / Medium impact**
- Personnel training
- ESP (remote access)
- PSP
- System security mgmt
- **Cyber security incident reporting & response**
- BCS recovery
- Change mgmt
- Vulnerability assessments
- Information protection
- CIP exceptional circumstances

**Low impact**
- Cyber awareness
- **Electronic Access Controls**
- Physical Security Controls
- Cyber security incident response
- **Transient cyber assets (TCA) risk mitigation**
- CIP exceptional circumstances
CIP-005-6
Effective Date of Standard 7/1/2020

Cyber Security — Electronic Security Perimeter(s)

**ESP**
- BCAs using routable protocols inside of ESP
- External routable connectivity through EAP
- **Implicit deny with documented whitelisting**
- Authentication on dial-up
- Visibility inbound/outbound communications

**Remote Access Mgmt**
- Utilize interface system / no direct access to BCA
- Encryption that terminates at intermediate system
- Multi-factor authentication
- **Logging & management of vendor remote access sessions**
CIP-010-3
Effective Date of Standard 7/1/2020
Cyber Security — Configuration Change Management and Vulnerability Assessments

Change Mgmt
- Establish baseline configs
- Authorize & document deviating configs within calendar 30 days
- Verify software integrity
- TEST configs

Configuration Monitoring
- Monitor every 35 calendar days for changes

Vulnerability Assessments
- Assess every 36 months and mitigate any gaps
- Exceptions could be replacement of same asset
CIP-013-1
Effective Date of Standard 7/1/2020
(NEW STANDARD)

• **Cyber Security — Supply Chain Risk Management**

  Documented supply chain cyber security risk management plan(s):
  - High & Medium BES Cyber Systems
  - Identify & assess vendor cyber risk(s) to the BES

  Documented supply chain cyber security risk management plan(s)

  CIP senior manager or delegate approve and revisit every 15 calendar months
CIP-008-6
Effective Date of Standard 1/1/2021

Cyber Security — Incident Reporting and Response Planning

Incident Response Plan
• Plan(s) to identify, classify, and respond to cyber events
• Is the event reportable or attempt at compromise
• Roles and responsibilities

Plan Testing & Updating
• Drill / test every 15 calendar months
• Update lessons learned 90 calendar days after drill testing
• Update roles changes within 60 days

Incident Reporting
• Reportable cyber event(s) notifications and updates include but not limited to E-ISAC and NCCIC
Questions

Cecil Elie
NPCC Senior CIP Analyst
celie@npcc.org
Root Cause Analysis of CIP Audit

Findings

Michael Stuetzle
Senior CIP Analyst
Objective

Analyze the root causes of CIP findings to provide focused and risk-based guidance to registered entities on the various reasons and aspects behind the findings.
Scope

• Compile CIP audit findings from January 1, 2017 to October 1, 2019 including PNCs and AOCs.
  – included all applicable CIP Standards
    • CIP-002-5.1, CIP-003-6, CIP-004-6, CIP-005-5, CIP-006-6, CIP-007-6, CIP-008-5, CIP-009-6, CIP-010-2, CIP011-2, CIP-014-2
Method

• Reviewed audit reports and enforcement documentation for AOCs and PNCs, and compiled into a single list

• Utilized NERC Cause Code Assignment Process to categorize and classify root causes for initial analysis

• Mapped the NERC Cause Code Assignments to the NPCC complied list of root causes.

An *anonymized* detailed analysis report will be available in November 2019
NERC Cause Coding

The purpose of cause coding is to provide a structured, measurable, and continuously improvable approach to rationally characterize the causes of reportable events so that the resulting information might be applied to develop actionable BPS risk reduction knowledge.

### NERC Cause Coding

<table>
<thead>
<tr>
<th>Category</th>
<th>Codes</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>A1 Design/Engineering</td>
<td>B1 Design Input</td>
<td>B1 Calibration for Instrumentation</td>
</tr>
<tr>
<td>A2 Equipment/Material</td>
<td>B1 Skill Based Error</td>
<td>B2 Equipment Failure to Perform</td>
</tr>
<tr>
<td>A3 Individual Human Performance</td>
<td>B1 Management Methods</td>
<td>B4 Supervisory Methods</td>
</tr>
<tr>
<td>A4 Management/Organization</td>
<td>B1 Written Communications Content</td>
<td>A5 Communication</td>
</tr>
<tr>
<td>A5 Communication</td>
<td>B1 Written Communications Presentation</td>
<td>A6 Training</td>
</tr>
</tbody>
</table>

### NERC CCAP Cause Code Quick Reference

[NERC CCAP Cause Code Quick Reference](#)
NPCC Cause Coding

<table>
<thead>
<tr>
<th>Code #</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Lack of documentation relation to a sale or organizational transition.</td>
</tr>
<tr>
<td>2.</td>
<td>Lack of awareness of compliance obligations.</td>
</tr>
<tr>
<td>3.</td>
<td>Lack of understanding of phased-in Implementation Plans.</td>
</tr>
<tr>
<td>4.</td>
<td>Ineffective policies or procedures.</td>
</tr>
<tr>
<td>5.</td>
<td>Ineffective or lack of proper controls.</td>
</tr>
<tr>
<td>6.</td>
<td>Ineffective management planning and verification.</td>
</tr>
<tr>
<td>7.</td>
<td>Processes that lack redundancy – single point of failure.</td>
</tr>
<tr>
<td>8.</td>
<td>Ineffective interdepartmental coordination. (i.e. silos)</td>
</tr>
<tr>
<td>9.</td>
<td>Ineffective workflow management.</td>
</tr>
<tr>
<td>10.</td>
<td>Insufficiently detailed procedures or expectations in documented procedures.</td>
</tr>
<tr>
<td>11.</td>
<td>Lack of proper documentation.</td>
</tr>
<tr>
<td>12.</td>
<td>Lack of proper training.</td>
</tr>
<tr>
<td>13.</td>
<td>Poor or nonexistent secondary reviews.</td>
</tr>
</tbody>
</table>
Analysis Summary

Number of CIP Audits analyzed: 43
  • Onsite: 21
  • Offsite: 22

Number of PNCs and AOCs found: 75
  • PNC: 37
  • AOC: 38
### Root Cause / CIP Standards Summary

#### Count per NPCC Cause Code

<table>
<thead>
<tr>
<th>NPCC Cause Code</th>
<th>Count of PNC/AOC</th>
</tr>
</thead>
<tbody>
<tr>
<td>2</td>
<td>22</td>
</tr>
<tr>
<td>6</td>
<td>16</td>
</tr>
<tr>
<td>10</td>
<td>14</td>
</tr>
<tr>
<td>5</td>
<td>8</td>
</tr>
<tr>
<td>9</td>
<td>5</td>
</tr>
<tr>
<td>7</td>
<td>4</td>
</tr>
<tr>
<td>14</td>
<td>3</td>
</tr>
<tr>
<td>1</td>
<td>2</td>
</tr>
<tr>
<td>11</td>
<td>1</td>
</tr>
</tbody>
</table>

#### Count per Standard

<table>
<thead>
<tr>
<th>CIP Standard</th>
<th>Count of PNC/AOC</th>
</tr>
</thead>
<tbody>
<tr>
<td>CIP-005</td>
<td>20</td>
</tr>
<tr>
<td>CIP-010</td>
<td>19</td>
</tr>
<tr>
<td>CIP-007</td>
<td>13</td>
</tr>
<tr>
<td>CIP-002</td>
<td>9</td>
</tr>
<tr>
<td>CIP-003</td>
<td>7</td>
</tr>
<tr>
<td>CIP-011</td>
<td>5</td>
</tr>
<tr>
<td>CIP-004</td>
<td>1</td>
</tr>
<tr>
<td>CIP-008</td>
<td>1</td>
</tr>
</tbody>
</table>

**Top 3 root causes account for almost 70% of all PNCs and AOCs**
Top 3 Root Causes - #1

NPCC Cause Code: 2
2) Lack of awareness of compliance obligations.

EA Cause Code: A3B2C05
A3 → Individual Human Performance
B2 → Rule Based Error
C05 → Delay in time caused LTA actions
Lessons Learned

NPCC Cause Code: 2

• Lack of awareness of compliance obligations
  – Create internal control to update documentation
  – Review and reference the NERC Glossary of Terms
  – Perform Mock Audits to the language of the standard, reference the RSAW
  – Train staff on Compliance Role / Responsibility
Top 3 Root Causes - #2

NPCC Cause Code: 6
6) Ineffective management planning and verification.

EA Cause Code: A4B4
A4 ➔ Management / Organization
B4 ➔ Supervisory Methods LTA
Lesson Learned

NPCC Cause Code 6

• Ineffective management planning and verification
  – Train management on Compliance Oversight responsibilities
  – Conduct periodic review of details required to maintain Compliance
  – Implement process to enforce company policies and procedures
Top 3 Root Causes - #3

**NPCC Cause Code:**
10) Insufficiently detailed procedures or expectations in documented procedures.

**EA Cause Codes:** A5B1/A5B2/A5B3

- A5 → Communication
- B1 → Written communications method of presentation LTA
- B2 → Written communication content LTA
- B3 → Written communication not used
Lessons Learned

NPCC Cause Code 10

• Insufficiently detailed procedures or expectations in documented procedures
  – Ensure processes in place to comply with the requirement are clearly documented
  – Ensure documentation covers each requirement part
  – Where possible, review documentation with an outside group for added perspective
Summary

• Reviewed all audit reports from January 2017 to October 2019
• Compiled PNCs and AOCs into a spreadsheet
• Analyzed findings for root cause trends
• Will be releasing an anonymized report in November with guidance to prevent occurrence/reoccurrence
• November 26 Webinar will be held to present the report to NPCC Stakeholders
• Final report will be given to the CC in December
Questions?
jvallace@npcc.org
jjimenez@npcc.org
mstuetzle@npcc.org
celie@npcc.org
Root Cause Analysis of O&P Enforcement
Objective

• Assign root cause categories to all Q1 and Q2 2019 noncompliance.
Events Analysis Cause Codes
NPCC Common Root Causes

1) Lack of documentation relation to a sale or organizational transition.
2) Lack of awareness of compliance obligations.
3) Lack of understanding of phased-in Implementation Plans.
4) Ineffective policies or procedures.
5) Ineffective or lack of proper controls.
6) Ineffective management planning and verification.
7) Processes that lack redundancy – single point of failure.
8) Ineffective interdepartmental coordination. (i.e. silos)
9) Ineffective workflow management.
10) Insufficiently detailed procedures or expectations in documented procedures.
11) Lack of proper documentation.
12) Lack of proper training.
13) Poor or nonexistent secondary reviews.
14) Human performance failures.
Method

- Reviewed enforcement PNCs from Q1 and Q2 2019 and compiled into a single list
- Utilized NERC EA Cause Code Assignment Process to categorize and classify root causes for initial analysis
- Next phase will map the NERC Cause Code Assignments to the NPCC complied list of root causes.
The Problem

The Root Cause
The Root Cause
Takeaways

- Multiple contributing causes
- Gather a detailed picture
Takeaways

• Multiple contributing causes

• Gather a detailed picture

• Focus on controls
Rumble Strips

• We need to think of problems with an assumption that humans will fail

• So our processes and systems need to engineer the solutions

• Change everything around people – processes and procedures
Root Cause Analysis

• Root cause analysis is all about perspective
• Understand the context
• Organizational weaknesses and procedural failures lead to most issues
• Focus on proper controls
• Think about causes like a system
NPCC Review Summary

• Reviewed all processed PNCs in Q1 and Q2 2019
• Compiled data for analysis
• Too early for larger conclusions
• Building data set for analysis to determine trends in the future
EA Cause Code Categories

A1 – Design / Engineering

A2 – Equipment / Material

A3 – Individual Human Performance

A4 – Management / Organization
EA Cause Code Categories

A5 – Communications

A6 – Training

A7 – Other
### Root Cause Standards Summary

<table>
<thead>
<tr>
<th>Cause Code Category</th>
<th>% of PNC</th>
<th>O&amp;P Standard</th>
<th>% of PNC</th>
</tr>
</thead>
<tbody>
<tr>
<td>A1 – Design / Engineering</td>
<td>4%</td>
<td>MOD-025-2</td>
<td>30%</td>
</tr>
<tr>
<td>A2 – Equipment / Material</td>
<td>2%</td>
<td>PRC-019-2</td>
<td>18%</td>
</tr>
<tr>
<td>A3 – Individual Human Performance</td>
<td>4%</td>
<td>PRC-024-2</td>
<td>14%</td>
</tr>
<tr>
<td>A4 – Management / Organization</td>
<td>83%</td>
<td>PRC-005-6</td>
<td>8%</td>
</tr>
<tr>
<td>A5 – Communication</td>
<td>2%</td>
<td>FAC-008-3</td>
<td>6%</td>
</tr>
<tr>
<td>A6 – Training</td>
<td>0</td>
<td>VAR-002-4</td>
<td>4%</td>
</tr>
<tr>
<td>A7 – Other</td>
<td>0</td>
<td>Rest</td>
<td>20%</td>
</tr>
</tbody>
</table>

Top root cause accounted for 36% of all PNCs;
# Most Common Root Causes - #1

**A4B1C01 – 36%**

A4 – Management / Organization

B1 – Management Methods Less than Adequate (LTA)

C01 - Management policy guidance or expectations are not well-defined, understood, or enforced.

**Ex:** Misunderstood compliance deadlines/responsibilities

<table>
<thead>
<tr>
<th>O&amp;P Standard</th>
<th>% of PNC</th>
</tr>
</thead>
<tbody>
<tr>
<td>MOD-025-2</td>
<td>55%</td>
</tr>
<tr>
<td>PRC-024-2</td>
<td>22%</td>
</tr>
<tr>
<td>PRC-019-1 and PRC-019-2</td>
<td>16%</td>
</tr>
<tr>
<td>VAR-002-4</td>
<td>5%</td>
</tr>
</tbody>
</table>
Most Common Root Causes - #2

A4B4C02 – 14%

- **A4** – Management / Organization
- **B4** – Management Methods Less than Adequate (LTA)
- **C02** - Progress/status of task not adequately tracked

Ex: Lack of documentation/failure to track compliance.

<table>
<thead>
<tr>
<th>O&amp;P Standard</th>
<th>% of PNC/AOC</th>
</tr>
</thead>
<tbody>
<tr>
<td>EOP-004-2</td>
<td>28%</td>
</tr>
<tr>
<td>FAC-008-3</td>
<td>28%</td>
</tr>
<tr>
<td>MOD-025-2</td>
<td>28%</td>
</tr>
<tr>
<td>PRC-019-2</td>
<td>16%</td>
</tr>
</tbody>
</table>
Most Common Root Causes - #3

**A4B3 – 13.3%**

- A4 – Management / Organization
- B3 – Work Organization and Planning Less than Adequate (LTA)
- C-- - Not Applicable

Ex: Failure to consider compliance dates.

<table>
<thead>
<tr>
<th>O&amp;P Standard</th>
<th>% of PNC</th>
</tr>
</thead>
<tbody>
<tr>
<td>PRC-019-2</td>
<td>80%</td>
</tr>
<tr>
<td>PRC-024-2</td>
<td>20%</td>
</tr>
</tbody>
</table>
Use the data

1. Identify Noncompliance
   - Use trends to better predict and prevent noncompliance
   - Establish trends and patterns in Root Cause Data
   - Collect Root Cause Data

2. Identify Root Cause
Takeaways

• Multiple contributing causes

• Gather a detailed picture

• Focus on controls
Internal Compliance Program
Internal Compliance Program

• Commitment to compliance accountability at all levels
• Preventative, Detective, Corrective Controls
• Ability to identify, assess, and correct noncompliance
• Feedback loop to improve program
All-level commitment

- Top Level / Executive Management ownership
- Separate compliance department
- Involvement/knowledge/training by everyone
- Encouragement to submit compliance concern
- Independent monitoring and auditing
- Regular reporting to Executive/Board/Top level management
All-level commitment

Executive Level / Board of Directors

Compliance Department

Information Technology
Operations / Planning
Security
Internal Controls

- Preventative
- Detective
- Corrective
<table>
<thead>
<tr>
<th>Identify noncompliance</th>
</tr>
</thead>
<tbody>
<tr>
<td>Identify and communicate possible noncompliance.</td>
</tr>
<tr>
<td>Investigate facts surrounding an identified possible noncompliance.</td>
</tr>
<tr>
<td>If determine facts do not amount to noncompliance (e.g., follow-up, if any, for near misses), what happens?</td>
</tr>
</tbody>
</table>
Assess noncompliance

- Process to assess risk to reliability
- Identify root cause
- Communicate reliability risk to individuals affected by noncompliance
- Communicate root cause to individuals responsible for mitigation
Correct noncompliance

Communicate root cause to individuals responsible for mitigation

Communicate to NPCC (if noncompliance)

Trend-spotting (similar causes)

Senior Management involvement to evaluate and correct

Evaluate effectiveness of mitigation
ICP Feedback Loop

• Review Program Periodically
• Track process
• Incorporate new Standards

Internal Compliance Program
# NERC Website for Future Enforcement

https://www.nerc.net/standardsreports/standardssummary.aspx

<table>
<thead>
<tr>
<th>Standard Number</th>
<th>Title</th>
<th>Effective Date of Standard</th>
<th>Phased-in Implementation Date (if applicable)</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Critical Infrastructure Protection (CIP)</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>CIP-003-7</td>
<td>Cyber Security — Security Management Controls</td>
<td>1/1/2020</td>
<td></td>
<td></td>
</tr>
<tr>
<td>CIP-003-8</td>
<td>Cyber Security — Security Management Controls</td>
<td>1/1/2020</td>
<td></td>
<td></td>
</tr>
<tr>
<td>CIP-005-6</td>
<td>Cyber Security — Electronic Security Perimeter(s)</td>
<td>7/1/2020</td>
<td></td>
<td></td>
</tr>
<tr>
<td>CIP-008-6</td>
<td>Cyber Security — Incident Reporting and Response Planning</td>
<td>1/1/2021</td>
<td></td>
<td>Detail</td>
</tr>
<tr>
<td>CIP-010-3</td>
<td>Cyber Security — Configuration Change Management and Vulnerability Assessments</td>
<td>7/1/2020</td>
<td></td>
<td></td>
</tr>
<tr>
<td>CIP-013-1</td>
<td>Cyber Security — Supply Chain Risk Management</td>
<td>7/1/2020</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Interconnection Reliability Operations and Coordination (IRO)</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>IRO-002-6</td>
<td>Reliability Coordination – Monitoring and Analysis</td>
<td>1/1/2020</td>
<td>WECC Regional Variance added. None of the continent-wide requirements have changed.</td>
<td></td>
</tr>
<tr>
<td><strong>Personnel Performance, Training, and Qualifications (PER)</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>PER-000-1</td>
<td>Specific Training for Personnel</td>
<td>10/1/2020</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Protection and Control (PRC)</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>PRC-012-2</td>
<td>Remedial Action Schemes</td>
<td>1/1/2021</td>
<td>PRC-012-2 will replace PRC-015-1 and PRC-016-1, PRC-012-1, PRC-013-1 and PRC-014-1 are withdrawn the date PRC-012-2 goes into effect.</td>
<td></td>
</tr>
<tr>
<td>PRC-027-1</td>
<td>Coordination of Protection Systems for Performance During Faults</td>
<td>10/1/2020</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Enforceable On January 1, 2020

- PRC-026-1 – Relay Performance During Stable Power Swings (Requirements R2–R4)
- CIP-003-7 – Cyber Security — Security Management Controls
- TPL-007-3 – Transmission System Planned Performance for Geomagnetic Disturbance Events (Requirements R5, 5.1, 5.2, R9, 9.1, and 9.2)
PRC-026-1
R2, R3, R4

Enforceable January 1, 2020
PRC-026-1

• R1 is already in effect (as of January 1, 2018)
• R2, R3, and R4 go into effect January 1, 2020

• This standard looks at relay performance during stable power swings.
Two Types Power Swings

• Stable Power Swings - where generators do not slip poles and the system reaches a new equilibrium

• Unstable Power Swings – where the system does not recover synchronization with the rest of the system – and requires intervention
Only Stable Power Swings

R2

2.1 - Within 12 months of a notification for R1 – determine whether load-responsive relay meets criteria of Attachment B.

2.2 – Within 12 months of becoming aware of generator, transformer or transmission line tripped in response to power swing due to operation of its protective relay – determine if relay meets criteria of Attachment B.
Requirement 3

R3

• Within six months of learning that a protective relay does not meet Attachment B criteria –
  – Develop a Corrective Action Plan (CAP)
Requirement 4

R4

• Implement each CAP or update timetables until all actions are complete.
CIP-003-7
Security Management Controls

Enforceable on January 1, 2020
Comparison
CIP-003-6 Versus CIP-003-7

Version 6

R1.2 For its assets identified in CIP-002 containing low impact BES Cyber Systems, if any:

– 1.2.1. Cyber security awareness;
– 1.2.2. Physical security controls;
– 1.2.3. Electronic access controls for Low Impact External Routable Connectivity (LERC) and Dial-Up Connectivity; and
– 1.2.4. Cyber Security Incident response.

Version 7

R1.2 For its assets identified in CIP-002 containing low impact BES Cyber Systems, if any:

– 1.2.1. Cyber security awareness;
– 1.2.2. Physical security controls;
– 1.2.3. Electronic access controls; and
– 1.2.4. Cyber Security Incident response;
– 1.2.5. Transient Cyber Assets and Removable Media Malicious Code Risk Mitigation;
– 1.2.6. Declaring and responding to CIP Exceptional Circumstances.

CIP-003-7 (Enforceable January 1, 2020)
Attachment 1: New Section 5

• Added requirement to include a section concerning, “Transient Cyber Asset and Removable Media Malicious Code Risk Mitigation” in to an Entity’s documented cyber security plan.

Modified Attachment 1 and 2 to replace “Low Impact BES Cyber System Electronic Access Point (LEAP)” and “Low Impact External Routable Communication (LERC).”
CIP-003-8
Security Management Controls

Enforceable on April 1, 2020
Why is there a CIP-003 version 7 and 8 coming out in 2020?

- Reliability Standard CIP-003-7 improvement objectives:
  1. Clarify Obligations relating to Electronic Access Control for Low Impact BES Cyber Systems;
  2. Address security controls for transient electronic devices used at low impact BES Cyber Systems; and
  3. Require a policy for declaring and responding to CIP Exceptional Circumstances related to low impact BES Cyber Systems.

- Version 8 is NERC’s response to the Commission’s directive in Order No. 843 to develop modifications to the Reliability Standards to mitigate the risk of malicious code that could result from third-party transient electronic devices for low impact BES Cyber Systems.
Comparison
CIP-003-7 Versus CIP-003-8

Version 7 Attachment 1 Section 5
5.2 For Transient Cyber Asset(s) managed by a party other than the Responsible Entity, if any, the use of one or a combination of the following prior to connecting the Transient Cyber Asset to a low impact BES Cyber System (per Transient Cyber Asset capability):

- Review of antivirus update level;
- Review of antivirus update process used by the party;
- Review of application whitelisting used by the party;
- Review use of live operating system and software executable only from read-only media;
- Review of system hardening used by the party; or
- Other method(s) to mitigate the introduction of malicious code.

Version 8 Attachment 1 Section 5
5.2 For Transient Cyber Asset(s) managed by a party other than the Responsible Entity, if any:
5.2.1 Use one or a combination of the following prior to connecting the Transient Cyber Asset to a low impact BES Cyber System (per Transient Cyber Asset capability):

- Review of antivirus update level;
- Review of antivirus update process used by the party;
- Review of application whitelisting used by the party;
- Review use of live operating system and software executable only from read-only media;
- Review of system hardening used by the party; or
- Other method(s) to mitigate the introduction of malicious code.

5.2.2 For any method used pursuant to 5.2.1, Responsible Entities shall determine whether any additional mitigation actions are necessary and implement such actions prior to connecting the Transient Cyber Asset.
TPL-007-3 – Transmission System Planned Performance for Geomagnetic Disturbance Events

• Requirement 5 and Requirement 9 Effective on January 1, 2020

• Applicable Functional Entities
  – Each responsible entity as determined in Requirement 1
    • Each Planning Coordinator, in conjunction with its Transmission Planner(s), shall identify the individual and joint responsibilities of the Planning Coordinator and Transmission Planner(s) in the Planning Coordinator’s planning area for maintaining models, performing the study or studies needed to complete benchmark and supplemental GMD Vulnerability Assessments, and implementing process(es) to obtain GMD measurement data as specified in this standard.
R1 and R2 were effective as of July 1, 2019.

R5 and R9 are effective on January 1, 2020

R11 and R12 are effective on July 1, 2021

R6 and R10 are effective on January 1, 2022

R3, R4, and R8 are effective as of January 1, 2023
TPL-007-3 – Transmission System Planned Performance for Geomagnetic Disturbance Events

**Need to Know**

- R5 and R9 requires applicable entities to provide GIC Flow information specified in R6 and R10 to the TO and GO.
- The sub-requirements are inclusions to what the information needs.

**Need to Do**

- Prepare your entity to submit information to your TO and GO.
Internal Controls – Evaluation, Testing and Issues/Trends

NPCC Entity Risk Assessment (ERA) Group
Risks

The terms “Risk”, “Risk Mitigation”, “Risk Tolerance”, “Inherent Risk”, “Residual Risk” have been appearing in our vocabulary more frequently:

- Financial Risks
- Occupational Risks
- Safety
- Health/Medical
- Reputation
- Travel/Commuting
- Legal (Liability)
- Business Continuity/Operations
“Where there’s Risks, there should be Controls”

• Controls are used to mitigate the consequences of Risks
• Fully implemented controls (tested and monitored) help ensure consistent, rigorous achievement of goals in a timely manner.
• Controls are:
  • Procedures, Policies, Guides, Practices, Instructions, Studies
  • Spreadsheets, Databases, Lists, Passwords, Patches, Barriers, Work Management, Reminders
  • Staff, contractors; trained to do their jobs; certified if necessary; job description/prerequisites
Food for Thought

Even if you're on the right track, you'll get run over if you just sit there.
Recent Trends/Issues

• Audit Findings vs. Controls
  • Audits are focused on meeting the wording of the Requirement.
  • Lack of (or poor controls) may be noted by the Audit Team as an Area of Concern and/or Recommendations to develop/improve controls. Controls are “forward looking”.

• The ERO is expected to assess the controls that support compliance to the NERC Reliability Standards
Recent Trends/Issues

• Many Registered Entities don’t fully understand what constitutes controls (and testing of same) versus Audit evidence.

• Regional Entities are not consistent in their approach, timing, data requests for controls documentation, and deliverables.
  • NPCC provided the North American Generators Forum (NAGF) with a presentation (tutorial, clarification, personal example, specific examples for Generator Owners and Operators) at their annual 2019 meeting.

  https://www.npcc.org/Compliance/Entity%20Risk%20Assessment/ppt_NAGF_InternalControls_NPCC_BEng_101619a.pdf
Evaluation of Internal Controls

The **evaluation of internal controls (eic)** occurs whether or not the entity provides controls information in advance of the audit.

- If controls information is provided well in advance of the audit, NPCC will do testing and assessment of the controls and
  - Provide a table of suggestions to enhance the controls and
  - If warranted, recommend
    - Possibly reducing sampling of audit evidence or
    - Possibly deferring the audit of the requirement to Spot Check or Self-Certification at a later date
- All evaluation and testing information, including justification for deferrals/sampling reductions are documented in NPCC Workpapers.
The *evaluation of internal controls (eic)* occurs whether or not the entity provides controls information in advance of the audit.

- If controls information are **not** provided in advance of the audit, then (during the audit) NPCC will:
  - review audit submittals, ask control questions, review testing of entity controls and
  - provide suggestions to enhance the controls
  - During the Audit Team Lead’s Initial Audit Briefing call, the eic auditor may introduce him/herself and provide a high level overview of what the eic process entails and types of information requested.
Recent Trends/Issues

• Registered Entities don’t realize that NPCC is testing their controls during the *evaluation of internal controls* process (whether prior to, or during the audit)

Hey, did NPCC test your controls?

Hmm...I’m not sure.
Does NPCC Test Entity Controls?

YES. Absolutely!!!

Assessment Criteria
The CEA may use a binary effective/not effective method for assessing implementation effectiveness, or it may use a measured approach to assess internal control implementation. CEAs should have a documented methodology for assessing implementation, and this methodology may include, but is not limited to, the following:

- The automation of internal controls
- Compensating and supporting internal controls
- Registered entity identification of key controls
- The level of available internal control documentation
- Peer review of key controls within the registered entity
- Feedback on control design processes
- Registered entity’s internal review and testing of existing internal controls
Controls Questions and Testing

During the eic, NPCC may ask Controls related questions:

• What procedure(s) are used to support compliance?
  • Are the procedures current? How do you know the steps in the procedure have been performed in a timely manner?
  • What (“testing”) evidence can you provide to confirm the above? Looking for Emails, work management task status/closeout, meeting minutes, checklist, lessons learned, logs, attendance, system out-put, screenshots, real time witness testing.

• What tools are used to support compliance?
  • How do you know the tools are working properly?
  • Do you have evidence that the tool has been used when required?
  • What “testing” evidence can you provide?

• Who is applying the tools and procedures listed above?
  • Are the people using the tools and applying the procedure qualified, trained, authorized?
  • What (“testing”) evidence can you provide (qualifications, training records, job description)
Controls Questions and Testing

• Answers to NPCC’s Control related questions and evidence of testing are documented in NPCC eic Workpapers

• Suggestions to enhance controls will be provided in the entity’s Compliance Oversight Plan (COP) and Audit Report
Controls for Cyber Security Risks

NPCC Entity Risk Assessment (ERA) Group
“...the RISC recommends the highest priority be given to those risk profiles that have been identified as having the higher likelihood/higher impact.”

**Higher Likelihood, Higher Impact**
- **Cybersecurity Vulnerabilities (RP #9)**
- Changing Resource Mix (RP #1)
- BPS Planning (RP #2)
- Resource Adequacy (RP #3)
Identified Risks – Presentation Focus

• ERO Reliability Risk Priorities, February 2018
  • **Report Risk Profile #9: Cybersecurity Vulnerabilities (CV)**
    • **CV Risk #1** - Cybersecurity threats result from exploitation of both external and internal vulnerabilities:
      a) Exploitation of employee and insider access.
      b) Weak security practices of host utilities, third-party service providers and vendors, and other organizations.
      c) Unknown, undisclosed, or unaddressed vulnerabilities and exposures in cyber systems.
      d) Growing sophistication of bad actors, nation states, malicious actors and collaboration between these groups.
    • **CV Risk #4** - Technologies and Services
      a) Increased reliance on third party service providers and cloud-based services for BPS operations and support.
      b) Cybersecurity risks in the supply chain: software integrity and authenticity; vendor remote access; information system planning; and vendor risk management and procurement controls.

Each control should identify key elements that ensure effective and efficient operation:

- People
- Process
- Technology

Each of these elements should contain the following attributes:

- Development
- Implementation/Maintenance
- Continuous Improvement

Controls should be **both effective and efficient**. Development, implementation/maintenance and continuous improvement are critical.
Control Development

- **People** – Security Architecture, Security Operations, Purchasing, HR, Users, Governance, Audit
- **Process** – Security Policies, Security Architecture, Acquisition, Strategic Security Roadmap
- **Technology** – Acquisition Management

Control Flow: Development

- **People/Services**
  - Skills
  - Knowledge

- **Process**
  - Scope
  - Audit/Certifications
  - Desired Results

- **Technology**
  - Environment
  - Capability

**Control Specifications**

- People, Process, Technology

**Entity/Vendor Personnel**
- Third Party/Vendors/Cloud Services/Supply Chain
- Risk Management Controls
- Software Integrity and Authenticity
- Logging/Monitoring/Alerting
- Intelligence Gathering/Sharing
- Vulnerability Assessment & Exposure Management
- Security Incident Handling/Response

**Acquisition Strategy & Execution**
**Deployment Strategy & Execution**

Start

- Determine Requirements
  - Business
  - Others
  - Compliance

End

- PPT

- Duration of Personnel Need
Cybersecurity threats result from exploitation of both external and internal vulnerabilities:

### Exploitation of Employee and Insider Access
- Know who is accessing your systems.
- Systems should be restricted to only personnel who need access.
- Identify user ability to cause harm and potential to cause harm.
- Third Parties, Manage Services and Contractors.

### Weak Security Practices
Source of Security Practices:
- Internal Entity Security Practices
- Third-Party Providers/Suppliers
- Other Organization (e.g. Government, RCs).

Practices:
- E.g.: Vulnerability / Patch Management, Policy/Procedures, Deployed Encryption, Information security, Remote Access, Exposure Management, Procurement.

### Key Inputs for Control Design:
These elements should be considered for designing key controls for this risk.

### Growing Sophistication of External Threats
- Bad/Malicious Actors (disruptive, Hacktivist or financial gain attacks).
- Nation States.
- Threat vectors cyber/physical/combination.
- Intelligence Gathering Sources.
- Widely Available Tools.

### Unknown, Undisclosed, or Unaddressed Vulnerabilities and Exposures
- Vulnerability and Exposure Management.
- Entity Risks.
- Defense in Depth.
- Intelligence Gathering.
2018 RISC Report – Risk #1: External and Internal Vulnerabilities Controls

**Human Capital Controls**
- Personnel Risk Assessment/Background Checks
- Human Capital Skills
- Vendor and Third Party Risk Assessment
- Periodic reviews of personnel risks, access authorization and rights
- Interpersonal relationships
- Personnel annual reviews
- Job rotations for key positions.

**Technical Controls**
- System Monitoring
- Preventive and corrective Systems (Firewalls, Intrusion Detections/prevention, Anti Malware and White listing, Remote Access)
- Restricted Access
- Vulnerability Assessment & Exposure Management

**Processes Controls**
- Internal control evaluations
- Process and Technical Security Controls effectiveness and adherence review.
- Third Party Audits/Certifications of Service Provider (Fedramp, ISO IEC 2700, SSA 16)
- Contract and SLA Management
- Procurement Management

**Internal/External Threats Awareness**
- ES-ISAC
- NERC Alerts
- FBI/DHS/Local Police
- Third Party Vendors
- Other Utilities
- Entity Personnel

**Key Outputs for Control Design**
- ES-ISAC
- NERC Alerts
- FBI/DHS/Local Police
- Third Party Vendors
- Other Utilities
- Entity Personnel
2018 RISC Report Risk #1 – Control Flow: Implementation/Maintenance

Vulnerability Assessment & Exposure Management

Process – Vulnerability Assessment, Exposure Mitigation
Technology – Vulnerability Assessment Tools, Exercises

Start

Manage Vulnerabilities & Exposure

Potential Vulnerability Identified

Vulnerability & Exposure Analysis

Exposure Mitigated?

Remediation Plan

Tune Management Methods

Intrusion Detection

NO

YES

NO

YES

YES

NO

NO

YES

YES
2018 RISC Report – Cyber Risk #4: Technologies and Services:

Key Controls/Control Areas for this Risk:

- Vendor/Service Provider Risk Management and Procurement Controls
- Vendor Service Provider Assessment and Audits
- Intelligence Gathering/Sharing
- Security Incident Handling/Response
- Security Protection Systems
- Information System Planning
- Software Integrity and Authenticity
- Vulnerability Assessment & Exposure Management

These controls work together to reduce this risk.

**Vendor/Service Provider Risk Management and Procurement Controls**

- **People** – Procurement, Security Architecture, Security Operations Team, Audit/Compliance, Vendor/Supplier Resources/ System Administrators
- **Process** – Corporate Supply Chain Process, Contracts, RFPs, NDA’s,
- **Technology** – Remote Access Process, Cloud Service Provider Technical Protections, NIDS, HIDS

**Software Integrity and Authenticity**

- **People** – Security Architecture, Security Operations Team, System Administrators, Vendors
- **Process** – Software Validity Verification, Software Monitoring, Software Assessment, Software Deployment, Vulnerability Assessment
- **Technology** – Software Monitoring, Software Deployment, Vulnerability Assessment

**Intelligence Gathering/Sharing**

- **People** – Security Operations Team, Audit/Compliance, Vendors/Government
- **Process** – Intelligence Gathering/Evaluation/Sharing
- **Technology** – Intelligence Sharing Platforms/Services

**Security Incident Handling/Response**

- **People** – Security Architecture, Security Operations Team, Audit/Compliance, System/Network Administrators, Vendors
- **Process** – Identify, Contain, Eradicate, Recover, Improvement
- **Technology** – Investigation, SEIM, Evidence Preservation, System Images, Recovery, Exercises

**Remote Access**

- **People** – Security Architecture, System Administrators, End User, Security Operations Team,
- **Process** – Monitoring, Detection, Remote Access Procedures
- **Technology** – Remote access servers, Jump Host, Firewall rules

**Information System Planning**

- **People** – Security Architecture, System Administrators, End User, Security Operations Team, Audit/Compliance, Vendors
- **Process** – Corporate Requirements/policies, vendor polices and services
- **Technology** – Security, Tool/Service Workflow, Technology Knowledge

**Entity/Vendor Personnel**

- **People** – Security Operations Team, Human Resources, System Administrators, Users
- **Process** – Hiring/contracting Process, Contracts/NDAs, Skills/Knowledge, Employee Training Plan
- **Technology** – Background checks, Employee/Vendor Reviews, Employee training

**Vendor Service Provider Assessment and Audits**

- **People** – Security Architecture, System Administrators, Security Operations Team, Audit/Compliance, Vendors
- **Process** – Vulnerability Assessment, Exposure Mitigation, Vendor Assessments, Certification(s), Audits, FedRAMP (Cloud Services)
- **Technology** – Vulnerability Assessment Tools, Exercises, IDS, Electronic Architecture.
2018 RISC Report – Cyber Risk #4: Technologies and Services

Control Flow Development, Implementation/Maintenance, Continuous Improvement:

- Vendor/Service Provider Risk Management and Procurement Controls
- Entity/Vendor Personnel
- Intelligence Gathering/Sharing
- Information System Planning
- Security Incident Handling/Response
- Vulnerability Assessment & Exposure Management
- Software Integrity and Authenticity
- Remote Access

Development Flow

Implementation/Maintenance Flow

Continuous Improvement Flow
2018 RISC Report Risk #4 – Control Flow: Implementation/Maintenance

Software Integrity and Authenticity

**People** — Security Architecture, Security Operations Team, System Administrators, Vendors

**Process** — Patch Validity Verification, Patch Monitoring, Patch Assessment, Patch Deployment, Vulnerability Assessment

**Technology** — Patch Monitoring, Patch Deployment, Vulnerability Assessment

---

**Start**

1. **New Software Availability**
   - **Is the Software required?**
     - **Yes**
       - **Validate Software Source?**
         - **Valid**
           - **Validate Software Authenticity?**
             - **Valid**
               - **Software Deployment Process**
             - **Not Valid**
               - **Investigate/Respond/Manage/Mitigate**
         - **Not Valid**
         - **System Monitoring**
     - **No**
       - **Vulnerability Assessment & Exposure Management**

---

**System Monitoring**

**PASS**

**FAIL**
Control Continuous Improvement

**People** – Security Architecture, Governance, Executive
**Process** – Strategic Security Plan
**Technology** – Risk Management

![Control Flow Diagram](image-url)
2018 RISC Report – Best Practices Sources

- **CIPC SCWG** - [https://www.nerc.com/pa/comp/Pages/Supply-Chain-Risk-Mitigation-Program.aspx](https://www.nerc.com/pa/comp/Pages/Supply-Chain-Risk-Mitigation-Program.aspx)
- **NATF** – [http://www.natf.net/documents](http://www.natf.net/documents)
- **EEI Cyber & Physical Security** - [https://www.eei.org/issuesandpolicy/cybersecurity/Pages/default.aspx](https://www.eei.org/issuesandpolicy/cybersecurity/Pages/default.aspx)
- **IIA Bulleting:** Cloud Security, Insider Threats, and Third-Party Risk, August 2019 (Member Ship Required)
Summary

Key points to consider:

• Identify and document People, Process, Technology Key Controls/Control Areas

• Develop Control Flows for Development, Implementation/Maintenance and Continuous Improvement

• One size doesn’t fit all
Questions?

Email: ERA@NPCC.org
CIP-005-6 R2 – Remote Access Management

• Effective July 1, 2020
• Two new Parts of R2 that apply to:
  – High Impact BES Cyber Systems and their associated PCA
  – Medium Impact BES Cyber Systems with External Routable Connectivity and their associated PCA
CIP-005-6 R2, Part 2.4

• Have one or more methods for determining active vendor remote access sessions (including Interactive Remote Access and system-to-system remote access)
CIP-005-6 R2, Part 2.5

• Have one or more method(s) to disable active vendor remote access (including Interactive Remote Access and system-to-system remote access)
CIP-010-3
Configuration Change Management and Vulnerability Assessments

CIP-010-3

• This Standard only has a single a major change from Version 2.
• The addition of R1.6
Watering Hole Attack

• The addition of R1.6 is intended to defend against a security exploit where an attacker compromises a group by infecting websites that the group visits.

• Intended to reduce supply chain risk
Addition of R1.6

R1.6 – Prior to a change from the existing baseline for:

1) Operating Systems or firmware where no independent operating system exists, (1.1.1)
2) Any commercially available open-source application software intentionally installed (1.1.2)
3) Any security patches (1.1.5)

The entity must...
R1.6 – The entity must...

• R1.6.1. Verify the identity of the software source

• R1.6.2. Verify the integrity of the software obtained from the source.
Software Verification

• Verifying the identity of the software source and the integrity of the software obtained from the software source - is a key control in preventing the introduction of malware or counterfeit software.

  – Intended to reduce the likelihood that an attacker could exploit legitimate vendor patch management processes to deliver compromised software updates or patches to a BES Cyber System.

  – Provide controls for verifying the baseline elements that are updated by vendors. It is important to note that this is not limited to only security patches.
CIP-013-1
Supply Chain Risk Management

CIP-013-1 (Enforceable July 1, 2020)
CIP-013-1 – Supply Chain Risk Management

- Applies to Entities that have High and Medium Impact BES Cyber Systems
- Focuses on the following four security objectives:
  1. software integrity and authenticity;
  2. vendor remote access protections;
  3. information system planning; and
  4. vendor risk management and procurement controls.
CIP-013-1 – Supply Chain Risk Management

• R1 – Document a supply chain cyber security risk management plan
• R2 – Implement the plan
• R3 – Review the plan once every 15 months and have CIP Senior manager approval
Future expectations of CIP-013-1 Supply Chain Risk Management

• Address Electronic Access Control and Monitoring Systems (EACMS)
  – Different discussions about separating Electronic Access Control and Electronic Access Monitoring

• Address Physical Access Control Systems (PACS) and Protected Cyber Assets (PCA)
PRC-002-2
Disturbance Monitoring and Reporting Requirements

R2-R4 and R6-R11

Enforceable July 1, 2020
PRC-002-2 – Disturbance Monitoring and Reporting Requirements

Applies to PC, GO, TO

R1 and R5 enforceable July 1, 2016

Sequence of Event recording (SER)
Fault Recording (FR)
Dynamic Disturbance Recording (DDR)
• R2 addresses data specifications for SER data
• R3 and R4 address data specifications for FR data
• R6 through R9 address data specifications for DDR data
• R10 and R11 address synchronization of data and format of SER, FR, and DDR data
PRC-002-2

• July 1, 2020 - Entities shall be at least 50% compliant [with R2-R4, R6-R11]

• Additional 2 years for entities to be fully compliant or for entities that own only one identified BES bus, BES Element, or generating unit.
Questions?