Critical Infrastructure Protection Violation Themes

Ken McIntyre, North American Electric Reliability Corporation
Deandra Williams-Lewis, ReliabilityFirst
Holly Hawkins, SERC Reliability Corporation
Dave Godfrey, Western Electricity Coordinating Council
Compliance Committee Meeting
May 9, 2018
• Purpose
  ▪ Lessons Learned
    o Identify themes in violations of the Critical Infrastructure Protection (CIP) Standards
    o Suggest potential resolutions

• Collaboration
  ▪ RF, WECC, and SERC worked with registered entities to identify the themes and resolutions

• Second Edition
  ▪ First edition in 2015
*The graph represents the violations that concern the more significant CIP compliance program deficiencies.*
• Lack of awareness of entity’s capabilities, deficiencies, systems, and processes

• Recurring Causes
  ▪ Lack of vigilance
  ▪ Insufficient expertise
  ▪ Inadequate root cause analysis
  ▪ Lack of engagement with regulator
Failure to verify

- Entity advanced in terms of security practices
- Entity assumed its program was working as intended in certain business areas
- Patch management program in those areas suffered.

Improvement

- Entity focused on evaluating the quality of their reliability activities
- Leveraged cross-functional teams to ensure consistency in implementation
Theme - Disassociation

- Disassociating compliance from security by extension and reliability, resulting in diminished value or emphasis on compliance
• Compliance is the baseline level of what a registered entity needs to do to maintain security.
• Compliance should be a byproduct of an effectively implemented security program.
Root Causes

- CIP-014 -2 physical security delegated and overseen by facilities or operations personnel
- Use of minimal security measures and accepting risk

Actions Taken

- Outreach and education with entities
- Executive management is getting engaged to understand the scope of the issue
- Additional Transmission studies will be performed
- Create cross functional team to ensure that threats and vulnerabilities
Theme - Inadequate Tools

- Inadequate tools, ineffective use of tools, and overreliance on automation
Systemic Issues

- Improperly configured intrusion detection system and firewall rules
- Over-reliance on automated tools
- Over-reliance on consultants

Actions Taken

- Update firewall configuration
- Implement automated tools along with manual oversight processes
- Focused training with consultants and internal personnel
• Lack of coordination between departments, business units, and different levels of management

Vertical Silos (Between Business Units or Departments)

Horizontal Silos (Between Layers from the Top Down)
Theme - Organizational Silos

- Exec.
- Middle Manager
- Staff
Failed Compliance Program

- Entity’s compliance program developed by upper management
- Not practical when applied at operational level
- Lack of internal communication in developing program

 Improvement

- Entity focused on better communication among departments
- Communication improved from upper management down as well as from the operational level up
• Generally, significant CIP compliance program deficiencies are result of multiple causes that overlap and are interrelated

• Example
  ▪ Disassociation and Lack of Awareness
    ○ Lack of engagement and/or participation
    ○ Organizational barriers and overreliance on consultants

• Lessons learned from both sides

• Recommendations
• Outreach and Education
  ▪ Interactions and engagements with registered entities
  ▪ Standards & Compliance workshops
  ▪ Regional Webinars
  ▪ Newsletter articles
  ▪ Engagement of the CIPC

• FERC Lessons Learned
  ▪ Lessons identified from FERC ledP audits
  ▪ Aligns with the ERO themes

• References
  ▪ 2018 CIP Themes and Lessons Learned
  ▪ FERC lessons learned
Questions and Answers
Compliance Monitoring and Enforcement Program Quarterly Report
Q1 2018

Sonia Mendonça, Vice President, Deputy General Counsel, and Director of Enforcement
Ken McIntyre, Vice President of Standards and Compliance
Compliance Committee Meeting
May 9, 2018
Percentage of Noncompliance by Discovery Method in Q1 2018

- Self-Report, 78.2%
- Self-Certification, 12.4%
- Audit, 8.1%
- Spot-Check, 1.3%
### Table A.1: Mitigation Completion Status

<table>
<thead>
<tr>
<th>Time Frame</th>
<th>Required Mitigation</th>
<th>On-going</th>
<th>Progress Toward Goal</th>
<th>Threshold</th>
<th>Target</th>
<th>Progress Since Last Quarter</th>
</tr>
</thead>
<tbody>
<tr>
<td>2015 and Older</td>
<td>10209</td>
<td>11</td>
<td>99.9%</td>
<td>99%</td>
<td>100%</td>
<td>0.02%</td>
</tr>
<tr>
<td>2016</td>
<td>1155</td>
<td>168</td>
<td>85.5%</td>
<td>85%</td>
<td>90%</td>
<td>5.34%</td>
</tr>
<tr>
<td>2017</td>
<td>2014</td>
<td>1086</td>
<td>46.1%</td>
<td>70%</td>
<td>75%</td>
<td>10.68%</td>
</tr>
</tbody>
</table>

### Ongoing Mitigation by Discovery Year

- **2015 & Older**: 1%
- **2016**: 13%
- **2017**: 86%
Serious Risk – Excluding CIP V5/V6

Non-CIP and V1-V3 Serious Risk Violations
3-Year Rolling Average

Percentage of Violations with Serious Risk per 3-Year Period

Filing Years

1.6% | 1.4% | 1.9% | 1.4% | 2.1% | 4.9% | 4.4% | 3.0% | 3.6%

Target, 5%

Target

Serious risk (Non-CIP and V1-V3)
Similar Prior Conduct

Compliance History for Moderate and Serious Risk Noncompliance

<table>
<thead>
<tr>
<th>Filing Year</th>
<th>Moderate and Serious Risk Filed with Compliance History</th>
<th>Moderate and Serious Risk with Similar Conduct</th>
<th>Total Moderate or Serious Risk Filed</th>
</tr>
</thead>
<tbody>
<tr>
<td>2012</td>
<td>215</td>
<td>102</td>
<td>459</td>
</tr>
<tr>
<td>2013</td>
<td>172</td>
<td>96</td>
<td>529</td>
</tr>
<tr>
<td>2014</td>
<td>153</td>
<td>60</td>
<td>342</td>
</tr>
<tr>
<td>2015</td>
<td>141</td>
<td>110</td>
<td>284</td>
</tr>
<tr>
<td>2016</td>
<td>134</td>
<td>111</td>
<td>301</td>
</tr>
<tr>
<td>2017</td>
<td>103</td>
<td>48</td>
<td>219</td>
</tr>
<tr>
<td>2018</td>
<td>3</td>
<td>31</td>
<td>3</td>
</tr>
</tbody>
</table>
• Implementation Guidance
  ▪ Eight endorsed, one non-endorsed, and four currently under review
• The Compliance and Certification Committee (CCC) approved a new Pre-qualified Organization.
  ▪ EnergySec
Coordinated Oversight Program for MRREs

Percentage of MRREs under Coordinated Oversight by Lead RE:
- MRO, 21%
- Texas RE, 21%
- WECC, 10%
- NPCC, 2%
- SPP RE, 13%
- SERC, 8%
- RF, 25%
Program Alignment

- Program Alignment Items:
  - Twelve completed, and
  - Five in progress.
- Continued outreach in collaboration with CCC Alignment Working Group at Regional Entity workshops
Questions and Answers