CIP Version 5
Transition Guidance

September 4, 2014

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

• Introduction
• Critical Asset Identification Options
• Newly Identified Critical Assets
• Updated Critical Cyber Asset List
• Changes to Existing Critical Assets / Critical Cyber Assets
• Compliance Monitoring During the Transition Period
• Technical Feasibility Exceptions
Introduction

• The goal of the CIP V5 Transition Guidance is to:
  – Provide Responsible Entities an efficient and effective path to full compliance with the CIP Version 5 Reliability Standards by the effective (enforcement) date.
  – Provide Responsible Entities a way to maintain CIP Version 3 compliance while transitioning to Version 5 through a flexible compliance monitoring and enforcement approach during the transition period.
  – Allow Responsible Entities begin to operate in accordance with the CIP V5 Standards while the CIP V3 Standards are still mandatory and enforceable.
Introduction

• During the transition period, Responsible Entities may:
  – Continue to comply with all of the CIP V3 Standards, or
  – Begin transitioning to compliance with some or all of the CIP V5 Standards

• Regional Entities will perform expanded outreach to help Responsible Entities achieve full compliance with the CIP V5 Standards by the effective date.
  – Workshops
  – Webinars
  – On-site meetings / readiness reviews
Introduction

• NERC has developed a “Mostly Compatible” matrix linking each CIP V3 Requirement with its comparable CIP V5 Requirement.

• The matrix will:
  – Assist Responsible Entities in transitioning their CIP compliance program from V3 to V5.
  – Assist Regional Entities and Responsible Entities with compliance monitoring and enforcement during the Transition Period.

• Matrix is found on the NERC web site at:
  
  http://www.nerc.com/pa/CI/Documents/V3-V5%20Compatibility%20Tables.pdf
## Introduction

### Table: Comparison

<table>
<thead>
<tr>
<th>Version 1</th>
<th>Version 2</th>
</tr>
</thead>
<tbody>
<tr>
<td>Requirement 1</td>
<td>Requirement 1</td>
</tr>
<tr>
<td>Requirement 2</td>
<td>Requirement 2</td>
</tr>
<tr>
<td>Requirement 3</td>
<td>Requirement 3</td>
</tr>
</tbody>
</table>

### Notes:

1. Requirement 1 includes a new subrequirement that was not present in Version 1.
2. Requirement 2 has been updated to include a new action plan.
3. Requirement 3 has been restructured to improve clarity.

---

[Link to document](http://www.nerc.com/pa/CI/Documents/93-05%20Compatibility%20Tables.pdf)
Critical Asset Identification Options

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

- Option 2:
  - Responsible Entities that have already adopted the CIP V4 Critical Asset Criteria (CIP-002-4, Attachment 1), may continue to use the CIP V4 Critical Asset Criteria in lieu of maintaining a RBAM.
    - Adoption of the V4 Critical Asset Criteria must have occurred before August 12, 2014.
    - Critical Assets identified per criterion 1.4 (Blackstart Resources) and criterion 1.5 (Cranking Paths) will not be subjected to the CIP V3 Standards, but Transmission Operator Control Centers controlling cranking path assets will continue to be treated as Critical Assets.
    - Annually approve the adoption of the V4 Critical Asset Criteria.
Critical Asset Identification Options

• Option 3:
  – Responsible Entities may adopt the CIP V5 “High” and “Medium” Impact Rating Criteria (CIP-002-5.1, Attachment 1) to identify Critical Assets in lieu of maintaining a RBAM.
    ▪ May adopt the V5 Impact Rating Criteria at any time.
    ▪ May immediately apply the V5 Impact Rating Criteria to derive a new Critical Asset list.
    ▪ May immediately remove Critical Assets and associated Critical Cyber Assets from the Critical Asset list that do not satisfy any of the V5 High or Medium Impact Rating Criteria.
    ▪ Annually approve the adoption of the V5 Impact Rating Criteria.
Critical Asset Identification Options

• Applying the CIP V5 “High” and “Medium” Impact Rating Criteria:
  – Read each Criterion statement as Critical Asset evaluation criteria.
  – Do not consider BES Cyber Systems located at or associated with the assets described by the Criteria.
  – Any asset matching one or more “High” or “Medium” Impact Rating Criteria is a Critical Asset.
  – Any asset matching only a “Low” Impact Rating Criterion is a not a Critical Asset.
Critical Asset Identification Options

• Additional Guidance:

  – Responsible Entities adopting either the CIP V4 Critical Asset Criteria or the CIP V5 Impact Rating Criteria must adopt the Criteria in their entirety, subject to the caveats documented in the CIP V5 Transition Guidance.

  – Adoption of either the CIP V4 Critical Asset Criteria or the CIP V5 Impact Rating Criteria should be documented by a Memorandum of Record or other, similar memorialization. A documented RBAM is not required.

  – Responsible Entities must annually apply the CIP V3 RBAM or alternative CIP V4 or V5 Criteria to derive an updated Critical Asset list.
Newly Identified Critical Assets

- Adoption and application of either the CIP V4 Critical Asset Criteria or the CIP V5 Impact Rating Criteria will result in an updated Critical Asset list.
  - Most existing Critical Assets will continue to be Critical Assets.
  - Some Critical Assets will not satisfy the Criteria and can be immediately removed from the Critical Asset list.
  - New Critical Assets may be identified as a result of adopting and applying the Criteria.
    - Newly identified Critical Assets should be flagged on the updated Critical Asset list as resulting from applying the CIP V4 Critical Asset Criteria or the CIP V5 Impact Rating Criteria.
Updated Critical Cyber Asset List

- After updating the Critical Asset list, the performance of CIP-002-3, Requirement R3, will result in an updated Critical Cyber Asset list.

- Any newly identified Critical Cyber Assets associated with a newly identified Critical Asset will not be expected to come into compliance with the CIP V3 Standards.
  - Newly identified Critical Cyber Assets should be flagged on the updated Critical Cyber Asset list
  - Such Critical Cyber Assets will be taken straight to CIP V5 compliance per the CIP V5 Implementation Plan.
Updated Critical Cyber Asset List

- Critical Cyber Assets associated with removed Critical Assets may be immediately removed from the Critical Cyber Asset list.
  - Removed Critical Cyber Assets will immediately come out of the CIP V3 compliance program.
  - Such Cyber Assets will likely come back into the CIP compliance program under CIP V5 as Low impacting BES Cyber Systems.
  - Resumed compliance under CIP V5 will be pursuant to the CIP V5 Standards Implementation Plan.
Updated Critical Cyber Asset List

• Existing Critical Cyber Assets that remained on the Critical Cyber Asset list after adoption and application of the CIP V4 or V5 Criteria and subsequent performance of CIP-002-3, Requirement R3, shall remain in the CIP V3 compliance program through the Transition Period.
  – No lapse of CIP compliance is permitted.
  – CIP V3 compliance must be maintained subject to the provisions of the CIP V5 Transition Guidance.
  – Replacement Cyber Assets must be CIP V3 or V5 compliant upon commissioning.
Changes to Existing CAs/CCAs

• Consistent with the *CIP V3 Implementation Plan for Newly Identified Critical Cyber Assets and Newly Registered Entities* and the CIP V5 Implementation Plan, new and upgraded/replaced Critical Cyber Assets resulting from a planned change must be fully compliant upon commissioning.
  
  – During the Transition Period, compliance may be with either the CIP V3 or CIP V5 standards.
  
  – Examples include planned replacement of the SCADA/EMS and planned conversion from a non-routable to a routable protocol in a Transmission substation or generating plant.
Changes to Existing CAs/CCAs

• A planned change that elevates BES Cyber Systems to a higher categorization during the Transition Period must be compliant with the higher impacting CIP V5 requirements by the effective date of the requirement.
  – Example includes a planned increase in generation that results in a higher categorization of BES Cyber Systems at the Control Center.

• Unplanned changes will need to be compliant by the later of the CIP V5 Standards effective date or the Compliance Implementation date shown in the CIP V5 Implementation Plan
  – Examples include Criteria 2.3 and 2.6 notifications.
Compliance Monitoring During Transition Period

- On-site CIP compliance audits of Responsible Entities registered as Reliability Coordinators, Balancing Authorities, or Transmission Operators, and other Responsible Entities with Critical Cyber Assets will continue through the Transition Period.

- Off-site CIP compliance audits of Responsible Entities with no Critical Cyber Assets (other than Reliability Coordinators, Balancing Authorities, and Transmission Operators) are cancelled through the Transition Period.
  - Self-reports, spot checks, and self-certifications still allowed.
  - Audits of “off-site entities” may resume with CIP V5.
Compliance Monitoring During Transition Period

• Responsible Entities audited during the Transition Period may choose to be audited against the CIP V3 or CIP V5 Standards.
  – Election made on requirement-by-requirement basis.
  – Election may be made on a site-by-site basis.

• Request for Information will be issued 45 days prior to issuance of the 90-day audit notice (135 days prior to the audit).
  – SPP RE will issue a spreadsheet with selection options.
  – Entities will have 15 days to respond.
## Compliance Monitoring During Transition Period

<table>
<thead>
<tr>
<th>CIP Version 3</th>
<th>CIP Version 5</th>
<th>Select the column you wish to be audited on Ver. 3</th>
<th>Ver. 5</th>
<th>Ver. 3 and Ver. 5</th>
</tr>
</thead>
<tbody>
<tr>
<td>CIP-002-3 R1</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>CIP-002-3 R1.1</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>CIP-002-3 R1.2</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>CIP-002-3 R1.2.1</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>CIP-002-3 R1.2.2</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>CIP-002-3 R1.2.3</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>CIP-002-3 R1.2.4</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>CIP-002-3 R1.2.5</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>CIP-002-3 R1.2.6</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>CIP-002-3 R1.2.7</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>CIP-002-3 R2</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>CIP-002-3 R3</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>CIP-002-3 R3.1</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>CIP-002-3 R3.2</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>CIP-002-3 R3.3</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>CIP-002-3 R4</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>CIP-003-3 R1</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>CIP-003-3 R1.1</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>CIP-003-3 R1.2</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>CIP-003-3 R1.3</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>CIP-003-3 R1.4</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>CIP-003-3 R1.5</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>CIP-003-3 R1.6</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>CIP-003-3 R1.7</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>CIP-003-3 R1.8</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>CIP-003-3 R1.9</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Compliance Monitoring During Transition Period

- At audit, in-scope requirements will be initially evaluated per the Responsible Entity’s selection.
  - If CIP V5 selected and compliance with the V5 language is determined, the V5 compliance will be viewed as CIP V3 compliant and a “No Finding” will be issued.
  - If CIP V5 is selected and non-compliance with the V5 language is determined, the audit team will revert back to the CIP V3 language. If V3 compliance is determined, a “No Finding” will be issued.
  - If neither CIP V3 nor V5 compliance is determined, a “Possible Violation” or “Area of Concern” will be issued.
Compliance Monitoring During Transition Period

• If a CIP V5 Requirement is selected by the entity, a “Possible Violation” will not be found for any part of the Requirement that is unique to CIP V5.
  – The audit team will conduct outreach to help steer the Responsible Entity back on course to CIP V5 compliance.
  – An “Area of Concern” may be issued to document the future potential non-compliance issue.

• Example includes aspects of the annual security training requirements of CIP-004-5, Requirement R2, such as Requirement R2.1.4 (the visitor control program).
Compliance Monitoring During Transition Period

• While not specified by the CIP V5 Transition Guidance, Responsible Entities selecting the CIP V3 audit option will not eliminate a CIP V5 evaluation opportunity.
  – If the V3 option is selected and non-compliance is determined, the audit team will determine if the issue of non-compliance would also be a CIP V5 violation.
  – If CIP V5 has eliminated the non-compliant aspect of the CIP V3 requirement, the audit team will issue an “Area of Concern” and not a “Possible Violation.”
    ▪ Example includes lack of an Electronic Access Point for non-routable communications as required by CIP-005-3, Requirement R1.
Compliance Monitoring During Transition Period

• Mitigation of any Open Enforcement Actions during the Transition Period should focus on achieving full compliance with the “Mostly Compatible” CIP V5 Requirement.
  – This includes violations found prior to the August 12, 2014 release of the CIP V5 Transition Guidance that have not completed mitigation.
  – Full compliance with the CIP V5 Standards must be achieved by the CIP V5 effective date.
  – An unmitigated Open Enforcement Action cannot be used to extend the CIP V5 compliance date.
Technical Feasibility Exceptions

• Technical Feasibility Exceptions are still required for certain CIP V5 Requirements.
  – Existing TFEs carried forward for equivalent CIP V5 Requirements.
  – New TFEs required for CIP V5 Requirements with no equivalent V3 Requirement.
  – TFEs for CIP V3 Requirements with no equivalent V5 Requirement will be terminated upon the CIP V5 effective date.

• CIP V5 TFEs cannot be submitted before October 1, 2015 to allow time for required portal changes.
Technical Feasibility Exceptions

- TFEs under the CIP V3 Standards with equivalent CIP V5 Requirements (carry forward).

<table>
<thead>
<tr>
<th>CIP V3 Requirement</th>
<th>CIP V5 Requirement</th>
</tr>
</thead>
<tbody>
<tr>
<td>CIP-005-3 / R4</td>
<td>CIP-005-5 / R2 / Part 2.3</td>
</tr>
<tr>
<td>CIP-007-3 / R2.3</td>
<td>CIP-007-5 / R1 / Part 1.1</td>
</tr>
<tr>
<td>CIP-007-3 / R6.4</td>
<td>CIP-007-5 / R4 / Part 4.3</td>
</tr>
<tr>
<td>CIP-007-3 / R5.3.3</td>
<td>CIP-007-5 / R5 / Part 5.6</td>
</tr>
</tbody>
</table>
Technical Feasibility Exceptions

- New CIP V5 TFE-eligible Requirements with no equivalent CIP V3 Requirement (submit).

<table>
<thead>
<tr>
<th>CIP-005-5</th>
<th>CIP-006-5</th>
<th>CIP-007-5</th>
<th>CIP-010-1</th>
</tr>
</thead>
<tbody>
<tr>
<td>Requirement R1, Part 1.4</td>
<td>Requirement R1, Part 1.3</td>
<td>Requirement R5, Part 5.1</td>
<td>Requirement R1, Part 1.5</td>
</tr>
<tr>
<td>Requirement R2, Part 2.1</td>
<td></td>
<td>Requirement R5, Part 5.7</td>
<td>Requirement R3, Part 3.2</td>
</tr>
<tr>
<td>Requirement R2, Part 2.2</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Technical Feasibility Exceptions

- CIP V3 TFEs no longer required under CIP V5 (terminate).

<table>
<thead>
<tr>
<th>CIP-005-3</th>
<th>CIP-006-3</th>
<th>CIP-007-3</th>
</tr>
</thead>
<tbody>
<tr>
<td>R3.1</td>
<td>R1.1</td>
<td>R3.2</td>
</tr>
<tr>
<td>R3.2</td>
<td></td>
<td>R4</td>
</tr>
<tr>
<td></td>
<td></td>
<td>R5.3</td>
</tr>
<tr>
<td></td>
<td></td>
<td>R5.3.1</td>
</tr>
<tr>
<td></td>
<td></td>
<td>R5.3.2</td>
</tr>
<tr>
<td></td>
<td></td>
<td>R6</td>
</tr>
</tbody>
</table>
Helpful Resources

- **SPP RE training**
  - Past Webinar and workshops presentation materials
  - Video library
  - SPP RE monthly newsletter

- **NERC**
  - CIP V5 Standards and Implementation Plan
  - CIP V5 Transition Guidance
  - CIP V5 Transition Study Lessons Learned
SPP RE CIP Team

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