

# Project 2014-02 CIP V5 Revisions

May 2014 Standard Drafting Team (SDT) Meeting Summary  
May 27, 2014

**RELIABILITY | ACCOUNTABILITY**



- SDT finalized CIP version 5 revisions for initial comment and ballot on June 2
- Additional support materials in Progress:
  - RAI-IAC FAQ, including enforcement scenarios
  - NERC is developing CIP version 5 RSAWs to post concurrently by June 17
- Key Dates:
  - June 2 – Target date for initial comment and ballot posting
  - June 19 – NERC Webinar on RAI; SDT Webinar on the posted proposed revisions

- Finalized IAC removal from the Standards
- NERC presented preliminary draft RSAWs for CIP-002, CIP-007 and CIP-009. Expects all CIP-002 through CIP-011 complete by posting
- The NERC RSAW development team will continue work on the RSAWs to post for comment draft RSAWs for the CIP V5 Revisions Standards concurrent with the CIP V5 Revision Standards posting (expected posting date of June 17)
- NERC presented draft responses to the FAQs on IAC and RAI that the SDT provided earlier in the development process
  - The SDT offered reactions and agreed to review more fully to provide suggested edits within a week
  - NERC continues to seek constructive input from the SDT as NERC finalizes the compliance documents associated with the revised CIP V5 Standards

- Finalized the proposed CIP-003, R2 requirements now in a table format
- Discussed additional physical access requirements applying to Low Impact BES Cyber Systems at Control Centers
- Modified electronic access requirement to require reasons for each inbound and outbound rule to align more with CIP-005-5
- Modified incident response plan requirements to add more specific criteria more in line with CIP-008

- Finalized CIP-006, Requirement Part 1.10 and CIP-007 Requirement Part 1.2
- Removed the “alternative measures” descriptor for protecting nonprogrammable components outside a PSP to avoid TFE triggering language

- Finalized CIP-010 R4 language
- Discussed the merits of adding Transient Device Requirements for Low Impact and agreed the vulnerability to High and Medium impact BES Cyber Systems was addressed without additional obligations for Low Impact
- Modified CIP-004 Requirement Part 2.1 to specifically include training content on transient devices
- Removed security patch level from the initial authorization and specified security patches can either be maintained or checked prior to use.

- Effective Date - Later of April 1, 2016 or 3 months following regulatory approval
- Low Impact (CIP-003 R2) - Later of April 1, 2017 or 9 months following regulatory approval.
- Communication (CIP-006 Requirement Part 1.10) - Effective Date + 9 months for new High and Medium Impact BES Cyber Systems
- Transient Devices (CIP-010 R4) - Effective Date + 9 months
- Concepts from CIP version 5 implementation plan (i.e. new assets, periodic requirements) carry forward with revisions

- This slide deck and other information relative to the CIP V5 Revisions SDT may be found on the Project 2014-02 Project Page under Related Files
  - <http://www.nerc.com/pa/Stand/Pages/Project-2014-XX-Critical-Infrastructure-Protection-Version-5-Revisions-Related-Files.aspx>





**Thank you**