Black Start Resource and New CIP Standards
Objective

- Compare Compliance Impacts of CIP Version 4 and CIP Version 5 for Blackstart and other Restoration Resources
• Approved by FERC on April 19, 2012
• Scheduled to become effective in April 2014
• Chances are it will not go in effect as FERC approves Version 5 in near future
• Changes to Critical Asset Identification from current version 3: criteria contained in CIP-002-4 Attachment 1 – Critical Asset Criteria.
• Each Blackstart Resource identified in the Transmission Operator's restoration plan.

• The Facilities comprising the Cranking Paths and meeting the initial switching requirements from the Blackstart Resource to the first interconnection point of the generation unit(s) to be started, or up to the point on the Cranking Path where two or more path options exist, as identified in the Transmission Operator's restoration plan.
• FERC issued a NOPR in April 2013
• Invited comments, but FERC intends to approve Version 5
• Approval likely in 3rd or 4th quarter
• Shift from identifying Critical Cyber Assets to identifying BES Cyber Systems
• Expected Date for Mandatory Compliance Jan 2016
• Drafting team heard concerns over compliance costs for Restoration Assets
• Drafting team sought informal input from NERC’s Operating and Planning Committees
• In the final version filed with FERC, Restoration Assets such as Blackstart Resources and Cranking Paths are categorized as Low Impact Assets
Applicable requirements for Low Impact Assets

- An inventory, list, or discrete identification of low impact BES Cyber Systems or their BES Cyber Assets is **not** required.
- CIP –3 R 2- implement, in a manner that identifies, assesses, and corrects deficiencies, one or more documented cyber security policies that collectively address the following topics, and review and obtain CIP Senior Manager approval for those policies at least once every 15 calendar months:
  - CIP-003 R 2.1 Cyber security awareness
  - CIP-003 R2.2 Physical security controls
  - CIP-003 R2.3 Electronic access controls for external routable protocol connections and Dial-up Connectivity
  - CIP-003 R2.4 Incident response to a Cyber Security Incident