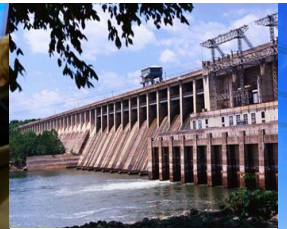
RELIABILITY FIRST

CIP-002-5.1 Audit Approach

Frank Kapuscinski, CISSP, MBA

Ron Ross, CISSP

October 2, 2015



General Audit Approach

- **How will we review your evidence?**
- **Have you evaluated all BES Assets and BES Cyber Assets?**

General Audit Approach

- **Audit to the Requirement Language and Applicability**
- **Use the following for guidance**
  - Guidelines and Technical Basis
  - V5 Transition Advisory Group Lessons Learned
  - V5 Transition Advisory Group Frequently Asked Questions

CIP-002-5.1 R1

➢ Measure

- Acceptable evidence includes, but is not limited to, dated electronic or physical lists required by Requirement R1, and Parts 1.1, 1.2 and 1.3.

➢ Verify that the entity's process:

1. Considers each of the asset types listed in R1 i through vi;
   i. Control Centers and backup Control Centers;
   ii. Transmission stations and substations;
   iii. Generation resources;
   iv. Systems and facilities critical to system restoration, including Blackstart Resources and Cranking Paths and initial switching requirements;
   v. Special Protection Systems that support the reliable operation of the Bulk Electric System; and
   vi. For Distribution Providers, Protection Systems specified in Applicability section 4.2.1 above.
2. Ensures that all assets of each applicable type are considered;
3. Identifies all high and medium impact BES Cyber Systems at each asset;
4. Assigns the correct impact rating to each identified high and medium impact BES Cyber System at each asset;
5. Identifies all assets which contain a low impact BES Cyber System.

CIP-002-5.1 R1

- **ReliabilityFirst uses Attachment C to review and select samples for audit**

- **Sampling**
  1. Assets which contain high and/or medium impact BES Cyber Systems.
  2. Assets which contain low impact BES Cyber Systems.
  3. Assets which do not contain BES Cyber Systems.
  4. High impact BES Cyber Systems.
  5. Medium impact BES Cyber Systems.
  6. List of all BES Cyber Assets included in high and medium impact BES Cyber System(s).
  7. List of all EACMS associated with high and medium impact BES Cyber Systems.
  8. List of all PCAs associated with high and medium impact BES Cyber Systems.
  9. List of all PACS associated with high and medium impact BES Cyber Systems.

- **Verify:**
  - High and medium impact BES Cyber Systems and/or BES Cyber Assets associated with the sampled asset(s) have been correctly identified and categorized.
  - Asset has been correctly identified as containing a low impact BES Cyber System.
  - The sampled asset does not contain a BES Cyber System.
  - The BES Cyber Assets comprising the high and/or medium BES Cyber System are identified.
  - The correct impact rating has been assigned to the BES Cyber System.

CIP-002-5.1 R2

- **Measure:**
  - Acceptable evidence includes, but is not limited to, electronic or physical dated records to demonstrate that the Responsible Entity has reviewed and updated, where necessary, the identifications required in Requirement R1 and its parts, and has had its CIP Senior Manager or delegate approve the identifications required in Requirement R1 and its parts at least once every 15 calendar months, even if it has none identified in Requirement R1 and its parts, as required by Requirement R2.

CIP-002-5.1 R2

➢ Verify:

- The reviews of the identifications in Requirement R1 have occurred at least every 15 calendar months during the audit period.
- The review of the identifications in Requirement R1 has occurred as required by "Implementation Plan for Version 5 CIP Cyber Security Standards."
- The approvals by the CIP Senior Manager or delegate of the identifications in Requirement R1 have occurred at least every 15 calendar months during the audit period.
- The approval by the CIP Senior Manager or delegate of the identifications in Requirement R1 has occurred as required by "Implementation Plan for Version 5 CIP Cyber Security Standards."

Questions & Answers

Forward Together ReliabilityFirst