

# NERC

NORTH AMERICAN ELECTRIC  
RELIABILITY CORPORATION

## CIP Standards Update

SANS Process Control & SCADA Security Summit  
March 29, 2010

Michael Assante  
Patrick C Miller

to ensure  
the reliability of the  
bulk power system

- FERC's Cyber Security Order 706 directed extensive modifications of CIP-002 through CIP-009 (Version 1)
  - Address the near term specific directives → Version 2
  - Address issues from FERC Approval of Version 2 (Sep 30, 2009) → Version 3
- Current Phase – Address remaining issues from FERC Order 706 and as raised by industry in the SAR → Version 4

# CIP Version 4 Key Guiding Principles

- The CIP Standards will:
  - Build on work already done complying with Version 1, including industry's experience and investment
  - Address the complex nature of BES functions and interconnected Cyber Systems, both within and between multiple organizations
  - Provide Entities with reasonable flexibility in applying equivalent security controls on the basis of compensating controls, cyber system characteristics, and operating environment considerations
  - Include all Cyber Systems with potential to adversely impact the reliability of the BES if lost, misused, or compromised

## Summary of CIP-002 Version 4

- All BES Subsystems identified and mapped to impact levels based on pre-determined criteria
  - Criteria for high, medium, and low impacts on Reliability Functions developed in collaboration with representatives of the CIP Standard Drafting Team, Operating Committee and Planning Committee
- All BES Cyber Systems identified and categorized with the highest impact level of its associated BES Subsystems
- Senior Manager approval of identification and categorization of BES Subsystems and BES Cyber Systems

# Differences Between Versions

## **Versions 1 / 2 / 3**

- Asset types to consider
- Critical Assets
- Critical Cyber Assets
- Critical / Not Critical
- “One size fits all” security

## **Version 4**

- Reliability Functions
- BES Subsystems
- BES Cyber Systems
- Impact Levels (High, Medium, Low)
- Security commensurate with BES reliability impact

# Recap of Activities

- “Version 2” Standards
  - Effective Date 4/1/2010
- “Version 3” Standards
  - Submitted to FERC
  - Awaiting Action by FERC
  - Will be effective start of 2<sup>nd</sup> ordinal quarter following approval
- “Version 4” Standards
  - Informal Comment Period on CIP-002-4d1

- CIP-002-4d1
  - 550 pages of comments submitted by industry for informal comment period
  - SDT reviewing and reacting to comments
  - Simplifying definitions and concepts
  - Relationship of CIP-002-4 with CIP-003-4 through CIP-009-4
  - Bright line thresholds for BES impact

- **CIP-003-4 through CIP-009-4**
  - “Bottom Up” vs. “Top Down”
    - I.e., start at ‘low’ impact
  - Relationship to existing work (ISA-99, NIST SP800-53, etc.)
  - Directives in FERC Order 706
  - Organization of requirements
    - Numbering of Version 4 standards
    - Formatting of multiple requirements statements for each requirement (e.g., H, M, L; Gen, Trans, CC; communications)

- Recent Phoenix Meeting
  - Preparing for next informal posting in May
  - Significant work on refining CIP-003-4 through CIP-009-4 requirements
    - 40-50% complete for posting
  - Further refinement of CIP-002-4
    - 80% complete for posting
  - Six sub-teams meeting weekly to prepare for next full meeting in April
  - Schedule for completion by end of year
    - Includes time for quality input from NERC Standards staff

- CIP-002-4 **NOT** to be filed separately in June 2010
- CIP-002-4 through CIP-009-4 filed (with FERC) together in December 2010
- Informal Comment Period for CIP-002-4 through CIP-009-4 scheduled to start early May 2010
- Technical Workshop by SDT in May
- Planning increased communications with the industry
- Formal Comment Period scheduled to begin in July 2010, with concurrent ballot pool formation
- Initial Ballot in September 2010
- Second ballot scheduled for October 2010
- File with regulators December 20, 2010

- FERC's recent position...
  - FERC approved process, but expressed concerns
  - Added CIP-006.R1.1 and CIP-007.R3
  - Questioned usefulness of Class-Based TFEs
  - Compensating measures must be equal or better security
  - Uniform Part A forms across all Regions
  - Concerned about potential abuse
- NERC issued Process Bulletin 2010-001

- CIP Version 4 is an important step towards a more holistic approach to BES cyber security
- Tiered security protection can target resources more effectively
- Industry stakeholder input and constructive comments are key to success of this industry effort to protect the cyber security of the BES

# For More Information

## Contacts:

### **Michael Assante**

Vice President and CSO  
NERC  
[michael.assante@nerc.net](mailto:michael.assante@nerc.net)

### **Patrick C Miller**

Technical Director  
CIP Practice, ICF International  
[pmiller3@icfi.com](mailto:pmiller3@icfi.com)