NERC Reliability Standards for Critical Cyber Assets

Sam Brattini, P.E.
November 2009

Background – FERC and the ERO

- Energy Policy Act 2005
  - FERC empowered to enforce mandatory compliance to Bulk Power System reliability standards
- July 2006: FERC appoints NERC the Electric Reliability Organization (ERO)
- FERC Order 693: FERC approves 83 NERC standards for mandatory compliance as of June 18, 2007
- Presently there are 95 approved standards

Reliability Standard Families

BAL	Resource and Demand Balancing	NUC	Nuclear
CIP	Critical Infrastructure Protection	ORG	Organization Certification
COM	Communications	PER	Personnel Performance, Training, and Qualifications
EOP	Emergency Preparedness and Operations	PRC	Protection and Control
FAC	Facilities Design, Connections and Maintenance	TOP	Transmission Operations
INT	Interchange Scheduling and Coordination	TPL	Transmission Planning
IRO	Interconnection Reliability Operations and Coordination	VAR	Voltage and Reactive
MOD	Modeling, Data, and Analysis		

Cyber Infrastructure Protection Standards

- Operations
  - CIP-001: Sabotage Reporting
- Cyber
  - CIP-002: Critical Cyber Asset Identification
  - CIP-003: Security Management Controls
  - CIP-004: Personnel and Training
  - CIP-005: Electronic Security Perimeter(s)
  - CIP-006: Physical Security of Critical Cyber Assets
  - CIP-007: Systems Security Management
  - CIP-008: Incident Reporting and Response Planning
  - CIP-009: Recovery Plans for Cyber Assets

KEMA

CIP Applicability

- Reliability Coordinator (RC)
- Balancing Authority (BA)
- Interchange Authority (IA)
- Transmission Service Provider (TSP)
- Transmission Owner (TO)
- Transmission Operator (TOP)
- Generator Owner (GO)
- Generator Operator (GOP)
- Load Serving Entity (LSE)
- NERC
- Regional Reliability Organizations

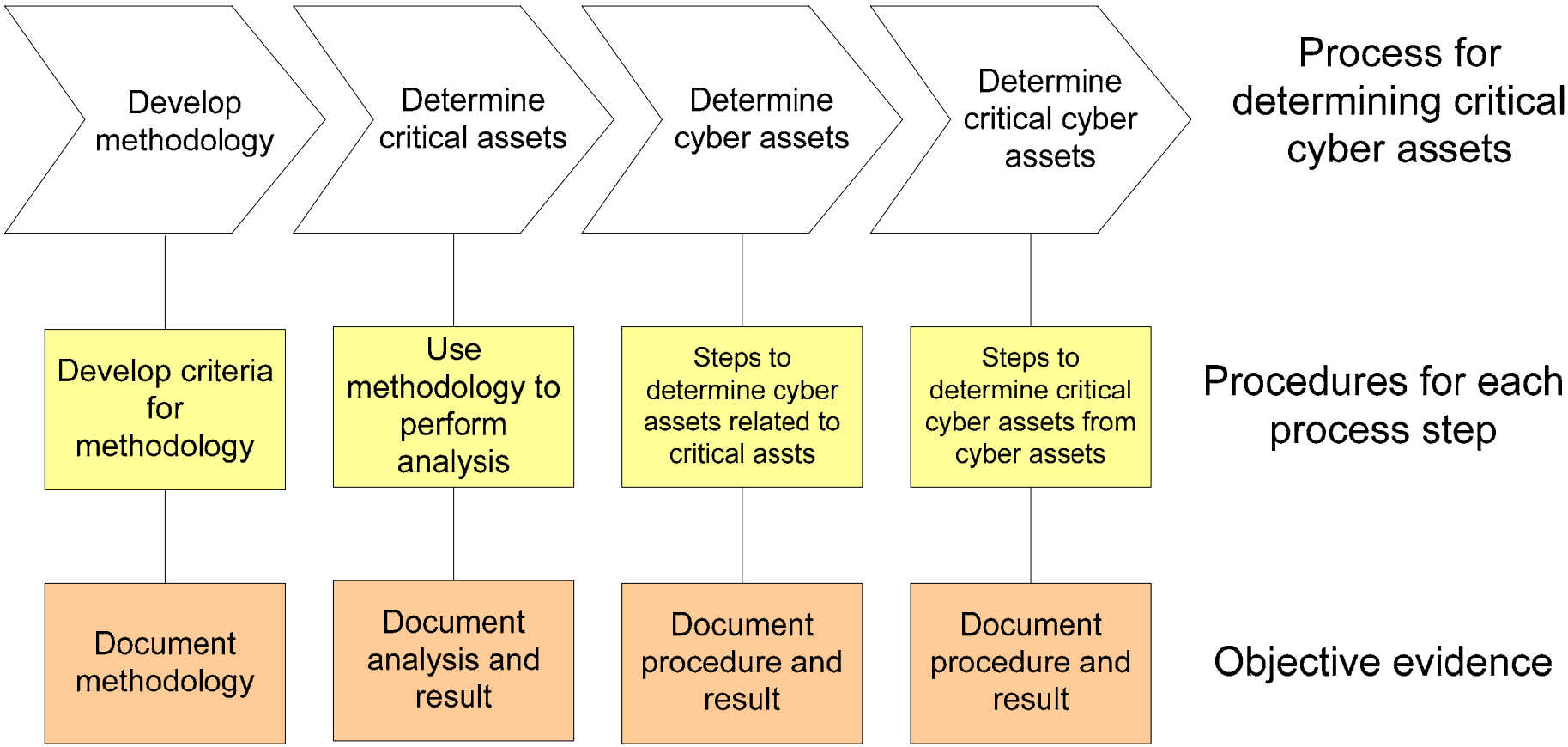
Applicability (continued)

- CIP-003 through CIP-009 are applicable only if critical cyber assets are identified as a result of satisfying the requirements of CIP-002.

- Null lists satisfy CIP-002 if applicable.

- Critical Asset
  - Facilities, systems, and equipment which, if destroyed, degraded, or otherwise rendered unavailable, would affect the reliability or operability of the Bulk Electric System.
  - Critical Cyber Assets are essential to the reliable operation of Critical Assets.

CIP-002, Determine Critical Cyber Assets



Significance of CIP Standards for Smart Grid

- Applicable for Bulk Electric System
  - Circuits operating above 100 kv
  - Primary and Backup Control Centers
  - Generation Resources
  - Transmission Substations
  - Special Protection Schemes
  - System restoration facilities
  - Automatic load shedding facilities

Questions???