NERC

NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

NERC Cyber Security Standards

SANS

January, 2008

Stan Johnson
Manager of Situation Awareness and Infrastructure Security
Stan.johnson@NERC.net
609-452-8060

to ensure the reliability of the bulk power system

Agenda

- History and Status of NERC Cyber Security Standards
- Applicable Entities
- Definitions
- High Level Overview of Standards Requirements
- Implementation Plans
- Implementation Schedule

Brief History of NERC Cyber Security Standards

- NERC Critical Infrastructure Protection Advisory Group (CIPAG) response to FERC request (5/9/02 to 7/31/02)
  - "Appendix G" of the FERC SMD NOPR
- NERC Urgent Action (UA) 1200 Standard
  - Temporary standard currently in place (approved 8/13/04)
  - Focus on Control Center
  - Authorized until August 2006
- NERC CIP Standards (formerly NERC 1300)
  - Recently Approved by Industry & NERC Board of Trustees
  - Permanent replacement
  - NERC 1200 & Substation & Power Plant

Drafting Process

- Standards Authorization Request:
  - Started on August 21, 2003
  - 2 drafts with industry comments
    - 95 pages of comments and responses
- Standard:
  - Started on June 8, 2004
  - 3 drafts with industry comments
    - 2580 pages of comments and responses
  - Ballot Version
    - 104 pages of comments and responses

Current Status

- Approved by industry:
  - Second Ballot complete March 24, 2006
  - 88.82% Approval by industry
- Approved by NERC Board of Trustees on May 2, 2006
  - “Effective Implementation” June 1, 2006
    - Implementation Schedule starts
- Submitted to FERC on August 28, 2006
  - Waiting for FERC action (Docket RM06-22)

Current Status

- Staff Assessment of CIP-002 through CIP-009
  - Issued December 12, 2006
  - Responses filed February 12, 2007
- FERC Final Rule
  - NOPR issued on July 20, 2007
  - Industry Comment filed by October 5, 2007
  - Final Rule Issued sometime “early” 2008

Future Status

- Final Rule will (likely) contain directed changes to standards
  - Clarify Requirements / Remove ambiguity
  - Include “implied” requirements
  - Some controversial issues
- Final Rule cannot change the standards language
  - Changes must go through Standards Development Process
  - Changes will therefore have their own implementation plan and schedule

Definitions

Definitions

- Critical Assets:
  - Facilities, systems, and equipment which, if destroyed, degraded, or otherwise rendered unavailable, would affect the reliability or operability of the Bulk Electric System.

Definitions

- Cyber Assets:
  - Programmable electronic devices and communication networks including hardware, software, and data.

Definitions

- Critical Cyber Assets:
  - Cyber Assets essential to the reliable operation of Critical Assets.

Definitions

- Bulk Electric System:
  - As defined by the Regional Reliability Organization, the electrical generation resources, transmission lines, interconnections with neighboring systems, and associated equipment, generally operated at voltages of 100 kV or higher. Radial transmission facilities serving only load with one transmission source are generally not included in this definition.

Definitions

- Adverse Reliability Impact:
  - The impact of an event that results in frequency-related instability; unplanned tripping of load or generation; or uncontrolled separation or cascading outages that affects a widespread area of the Interconnection.

Definitions

- Technical Feasibility:
  - **refers only to engineering possibility and is expected to be a "can/cannot" determination in every circumstance. It is also intended to be determined in light of the equipment and facilities already owned by the Responsible Entity. The Responsible Entity is not required to replace any equipment in order to achieve compliance with the Cyber Security Standards. When existing equipment is replaced, however, the Responsible Entity is expected to use *reasonable business judgment* to evaluate the need to upgrade the equipment so that the new equipment can perform a particular specified technical function in order to meet the requirements of these standards.**

(from the FAQ)

Definitions

- Reasonable Business Judgment:
  - **The phrase is in NERC Standards CIP-002 through CIP-009 to reflect — and to inform — any regulatory body or ultimate judicial arbiter of disputes regarding interpretation of these Standards — that Responsible Entities have a significant degree of flexibility in implementing these Standards.**
  - **This principle, however, does not protect an entity from simply failing to make a decision.**

(from the FAQ)

Definitions

- Significant Adverse Impact:
  - **With due regard for the maximum operating capability of the affected system, one or more of the following conditions arising from faults or disturbances, shall be deemed as having significant adverse impact:**
    - **System instability;**
    - **Unacceptable system dynamic response or equipment tripping'**
    - **Voltage limits in violation of applicable emergency limits;**
    - **Loadings on transmission facilities in violation of applicable emergency limits;**
    - **Unacceptable loss of load.**

(IEEE C37.100-1981)

Applicable Entities

- Reliability Coordinator
- Balancing Authority
- Interchange Authority
- Transmission Service Provider
- Transmission Owner
- Transmission Operator
- Generator Owner
- Generator Operator
- Load Serving Entity
- NERC Office *
- Regional Reliability Organization *

* Not part of NERC Functional Model

See http://www.nerc.com/~filez/functionalmodel.html

Not Applicable

- "Facilities regulated by the U.S. Nuclear Regulatory Commission or the Canadian Nuclear Safety Commission"
- Communications networks between discrete Electronic Security Perimeters
- Entities with no "Critical Cyber Assets" determined after complying with NERC Standard CIP-002
  - Must only annually comply with Standard CIP-002

General Concept

- Applying IT “thought concepts” to control network environment
  - Policy & Procedure
  - Access control
  - Security perimeters
  - Auditing
  - Change management
- Focus on Bulk Electric System “Critical Assets”
- Focus on “Critical Cyber Assets”
- Focus on “routable protocol” communications
- Process and documentation centric
  - Including annual reviews

NERC CIP Standards

- **CIP-002 – Critical Cyber Assets**
- **CIP-003 – Security Management Controls**
- **CIP-004 – Personnel and Training**
- **CIP-005 – Electronic Security**
- **CIP-006 – Physical Security**
- **CIP-007 – Systems Security Management**
- **CIP-008 – Incident Reporting & Response Management**
- **CIP-009 – Recovery Plans**

- **Implementation Plan**

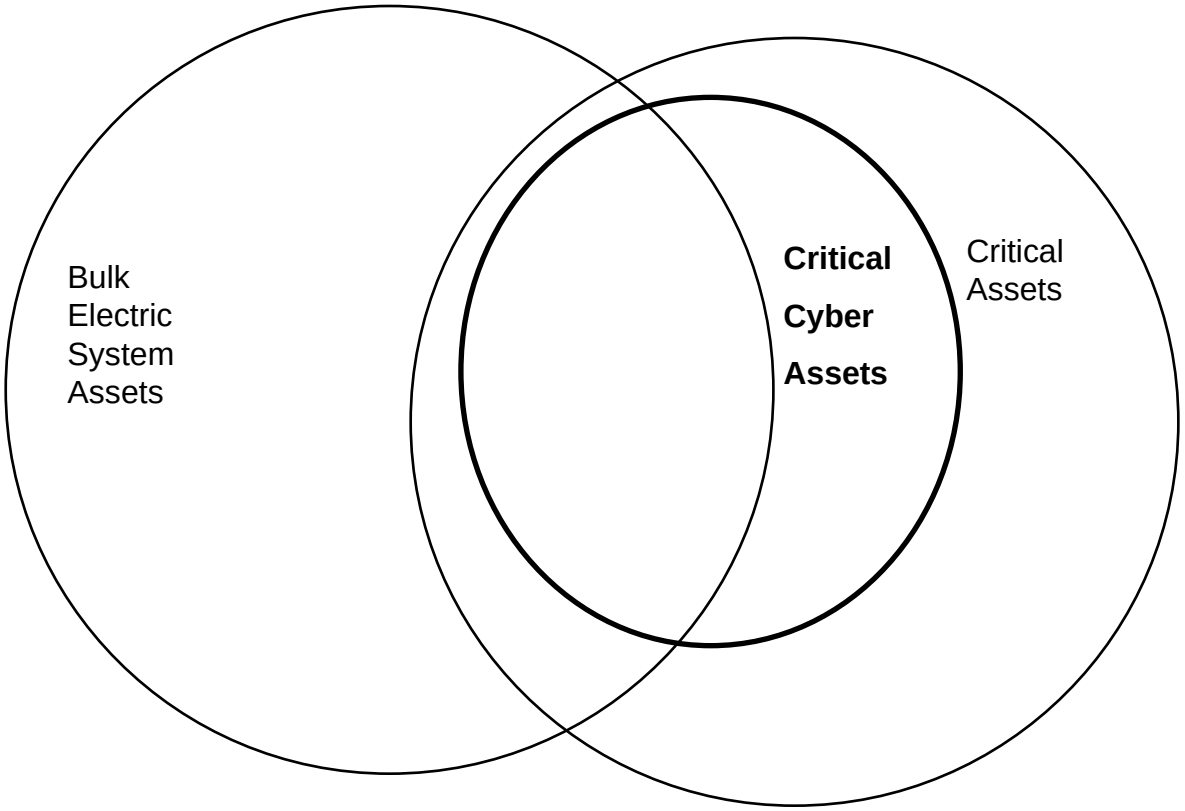
CIP-002 – Critical Cyber Assets

- **Derive list of Critical Assets**
  - **Risk-based approach**
  - ***Electrically critical for reliable BES operations***
- **Derive list of Critical Cyber Assets**
  - ***"Essential to the reliable operations"* of Critical Assets**
  - **Considerations for communications characteristics**
- **Senior Management approval**
  - **Annual review**
  - **May determine null set of Critical Cyber Assets**

Risk-Based Methodology

- Risk to Bulk Electric System – therefore an Impact Analysis
  - Must "consider":
    - **Control centers and backup control centers performing the functions of the entities listed in the Applicability section of this standard.**
    - **Transmission substations that support the reliable operation of the Bulk Electric System.**
    - **Generation resources that support the reliable operation of the Bulk Electric System.**
    - **Systems and facilities critical to system restoration, including blackstart generators and substations in the electrical path of transmission lines used for initial system restoration.**
    - **Systems and facilities critical to automatic load shedding under a common control system capable of shedding 300 MW or more.**
    - **Special Protection Systems that support the reliable operation of the Bulk Electric System.**
    - **Any additional assets that support the reliable operation of the Bulk Electric System that the Responsible Entity deems appropriate to include in its assessment.**

Critical Cyber Assets



Electric
System

CIP-003 – Security Management Controls

- Documented Cyber Security Policy
  - “control system specific”
- Senior Management responsibility
- Exception process defined
- Information classification & protection program
- Access control program
- Change control & configuration management program

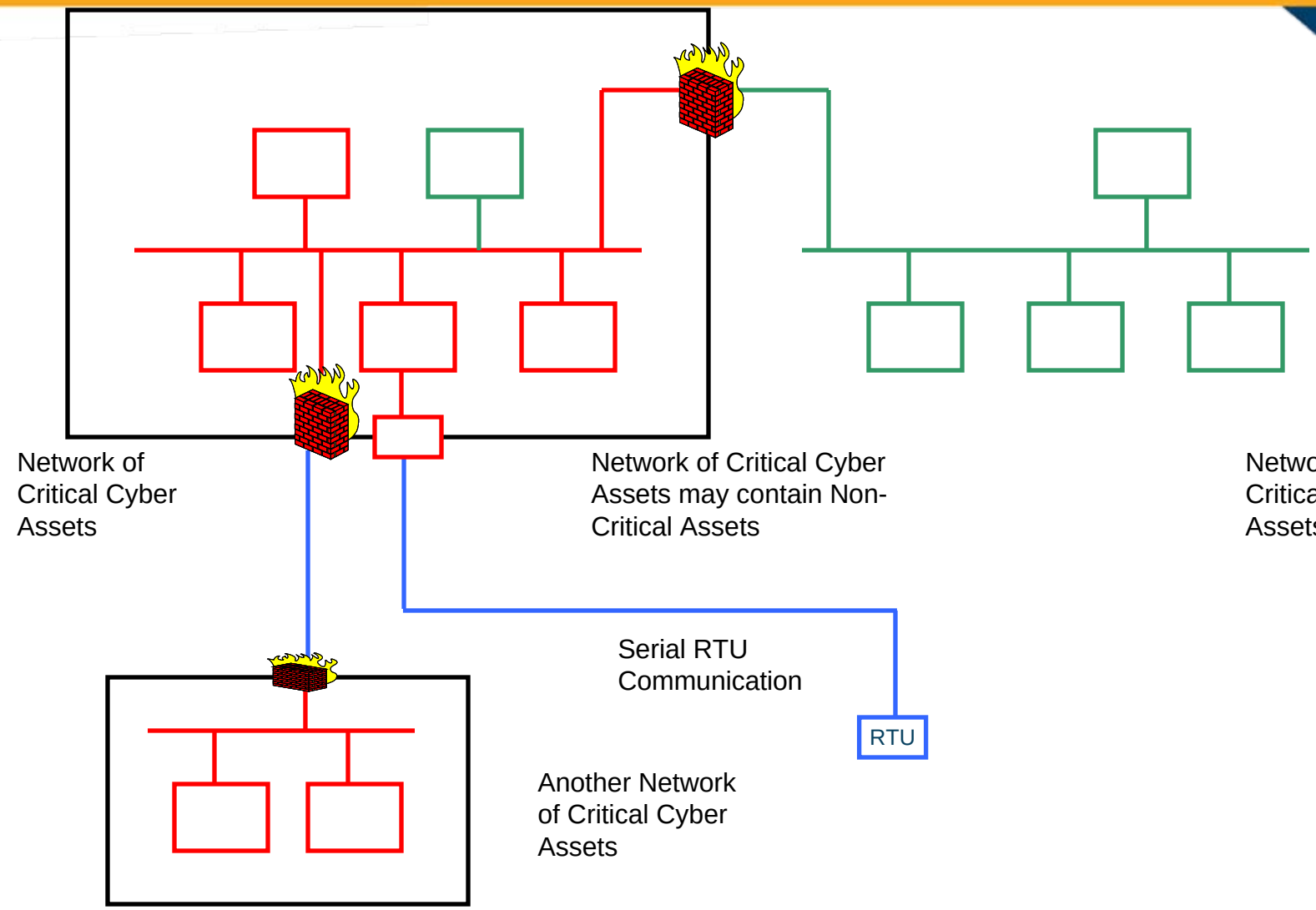
CIP-004 – Personnel and Training

- Awareness
  - Continual, informal, ongoing
- Training
  - Annual, formal, attendance records
- Personal Risk Assessment
  - a.k.a Background Checks
  - Management observation
- Access management
  - Approvals, records retention, termination
  - Escorted access

CIP-005 – Electronic Security

- Electronic Security Perimeter identification
  - Contains “all” Critical Cyber Assets
  - May have multiple Electronic Security Perimeters
  - May contain non-critical cyber assets
  - Access point identification & protection
- Electronic access controls
  - Access point protection
- Electronic access monitoring
  - Review access logs
- Cyber vulnerability assessment (of perimeter)

Electronic Security Perimeter



CIP-006 – Physical Security

- **Physical Security Plan with identified Physical Security Boundary**
  - **Must contain all Critical Cyber Assets**
  - **May have multiple Physical Security Perimeters**
- **Physical access controls**
  - **e.g., electronic card key**
- **Physical access monitoring**
  - **e.g., CCTV**
- **Physical access logging**
  - **e.g., card access log**
- **Access log retention and review**

CIP-007 – Systems Security Management

- Test Procedures for new systems and significant changes
- Disable unused & unneeded ports and services
- Security patch management
- Malicious software prevention
- Account management
- Security event & status monitoring
- Disposal or redeployment of Cyber Assets
- Cyber vulnerability assessment (of Cyber Assets)

CIP-008 – Incident Reporting & Response Management

- **Documented Cyber Security Incident Response Plan**
  - **Refer to NERC / ES-ISAC "Indications Analysis & Warning" (IAW) procedures**
  - **Currently under review by CIPC**
  - **Annual exercise of plan**
- **Incident documentation**
  - **Keep documentation relating to incidents, including logs, surveillance, investigations, recovery, reports, etc.**
  - **Special care if law enforcement and prosecution will be involved**

CIP-009 – Recovery Plans

- **Recovery plan documentation**
  - **For varying duration and severity**
  - **Defined roles and responsibilities**
- **Annual exercise of plans**
- **Update plans to reflect environment changes**
- **Backup, restore and secure storage of information**
- **Testing backup media**

Implementation Plan

- **Phased Plan**
- **4 (really 3½) "levels" of compliance:**
  - **"BW" – Begin Work**
    - **Entity has a plan to address requirements**
  - **"SC" – Substantially Compliant**
    - **Entity is implementing its plan**
  - **"C" – Compliant**
    - **Entity has completed technical work, but does not have a full year of required logs**
  - **"AC" – Auditably Compliant**
    - **Entity meets full requirements of standard – with all logs and records**

Implementation Plan

- **Four separate compliance schedule tables:**

  1) Balancing Authorities and Transmission Operators that *were* required to self-certify compliance to UA1200, and Reliability Coordinators

  2) Transmission Operators and Balancing Authorities that *were not* required to self-certify compliance to UA1200, along with Transmission Providers, and the Offices of NERC and the Regional Reliability Organizations

Implementation Plan

3) **All entities required to register to the Functional Model during calendar year 2006 (pursuant to the NERC / ERO filing activities).**

4) **All entities registering to a Functional Model function in 2007 and thereafter.**

- **Entities that currently do not "exist"**

Implementation Plan

- **Implementation Plan tables specified by CIP Standard and individual requirement**
- **4 years for all currently (2006) registered entities to reach "Auditable Compliant" (2007 to 2010)**
  - **Maximum of 3 years to complete work and achieve "Compliant" (2009)**
  - **Some requirements in Table 1 reach "Compliant" in 2008**