Status Report for

Critical Infrastructure Protection Advisory Group

Jim Brenton

Director, ERCOT Security

ERCOT Board of Directors Meeting

November 14, 2006

Background

- On May 2, 2006 NERC's Board of Trustees adopted 8 new Reliability Standards with respect to Cyber and Physical Security **effective June 1, 2006**.
- These new standards, along with CIP-001-0: Sabotage Reporting (effective April 1,2005) comprise NERC's Physical and Cyber Security standards and **replace the Urgent Action 1200 Standard.**
- The CIP Standards are applicable to ERCOT and a significant number of market participants.
- Implementation of the CIP Standards will be phased in over the next three years until entities reach Auditable Compliance for all CIP Standards.
- Expect Readiness Audits may commence starting in June 2007.

Key Standard for ERCOT:
CIP-002-1: Critical Cyber Asset Identification

Requirements:

- Identify & document a risk based assessment methodology to identify Critical Assets.
- Identify list of Critical Assets based on the risk based assessment methodology.
- Using list of Critical Assets, develop a list of associated Critical Cyber Security Assets essential to the operation of the Critical Asset.
- Senior management review and approval of list of Critical Assets and Critical Cyber Security Assets annually.

Applicability:

- Reliability Coordinator
- Balancing Authority
- Interchange Authority
- Transmission Service Provider
- Transmission Owner
- Transmission Operator
- Generation Owner
- Generation Operator
- Load Serving Entity
- NERC
- Regional Reliability Organizations

Exempt:

- Facilities regulated by the US Nuclear Regulatory Commission or the Canadian Nuclear Safety Commission.
- Cyber Assets associated with communication networks & data communication links between discrete Electronic Security Perimeters.

ERCOT’s Game Plan for Compliance

- **ERCOT staff and Market Participants have attended NERC sponsored workshops on the CIP standards.**
- **On November 1, ERCOT hosted a Cyber Security Workshop to facilitate discussion on CIP Standard’s requirements and compliance awareness.**
  - Focus on “How to get started” toward understanding the new standards and what does it take to get ready for compliance.
  - Technical discussion of Critical Asset determination within ERCOT.
  - Discussed relationship between Critical Cyber Assets and Critical Assets.
- **On November 2, ERCOT hosted an exploratory meeting with ERCOT Market Participants to determine if the ERCOT Critical Infrastructure Advisory Group (CIPAG) should be reactivated.**
  - In 2004, an original attempt at forming a ERCOT CIPAG did not proceed forward.
  - For 2006, Market Participants in agreement to move forward with a new CIPAG.
  - Developed a draft Mission Statement

2006 CIP Advisory Group

Purpose:

The ERCOT CIP Advisory Group would serve as a vehicle to facilitate and enable ERCOT entities to secure their critical assets, to become compliant, and to maintain compliance with relevant security standards.

To accomplish this, the ERCOT CIPAG will:

- Collaborative effort
- Discuss security solutions
- Share information
- Communicate and clarify relevant security standards
- Provide guidance in security standards implementation and compliance
- Provide a forum for CIP discussions with State and Federal authorities

2006 CIPAG Proposed Governance & Activities

Immediately form a temporary Steering Committee to:

- Recruit Membership.
- Draft a charter and propose a governance structure for review by the ERCOT Board of Directors (Q1-2007).

Concurrent Activities:

- Continue discussion of CIP standards and implementation issues:
  - Focusing on communication, assessment methodologies, and compliance.
  - Could possibly form subgroups if needed.
- Committee will meet again on December 4, 2006.
- Companies who have currently volunteered resources to the Steering Group:
  - ERCOT
  - Austin Energy
  - PUCT Staff
  - STEC
  - TXU Power
  - TXU Electric Delivery
  - City of Garland
  - Bryan Texas Utilities
  - CenterPoint
  - LCRA
  - TMPA
  - CPS

Questions

Additional Background Information

Key NERC Definitions

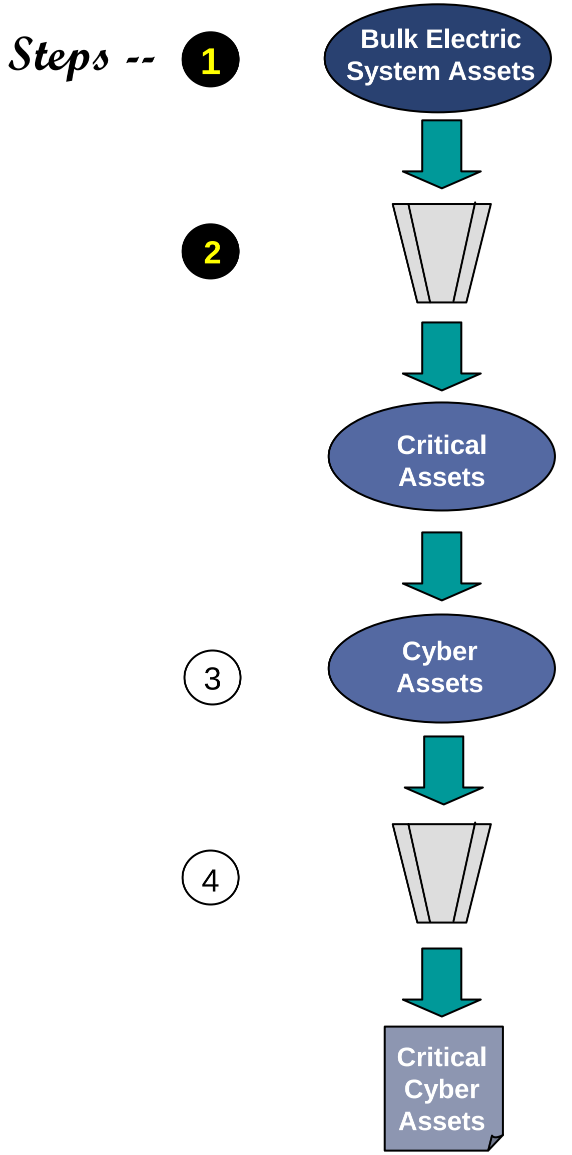
Bulk Electric System: The electrical generation resources, transmission lines, interconnections with neighboring systems, and associated equipment, generally operated at voltages of 100 kV or higher. Radial transmission facilities serving only load with one transmission source are generally not included.

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.

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

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

Critical Asset Selection Process



Steps -- 1

Bulk Electric System Assets

2

Critical Assets

Cyber Assets

3

4

Critical Cyber Assets

Inputs - List of generating resources; control centers & backup control centers; system restoration, automatic load shedding, & system protection assets, etc.

Filtering - Risk Based Assessment
(Required Document)

Output - List of Critical Assets
(Required Document)

This presentation will discuss only Steps 1 & 2

Inputs - Cyber assets supporting Critical Assets

Filtering - Essential to operation of critical asset **and** meet CIP 002 R3

Output - List of Critical Cyber Assets
(Required Document)

Step 1: Develop a List of Bulk Electric System Assets

Per CIP-002, R1.2; the following assets must be considered as input in ERCOT's risk based assessment:

- Control Centers and backup Control Centers;
- 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; and
- Any additional assets that support the reliable operation of the Bulk Electric System.