



# ERCOT Cyber Security Standards Workshop: CIP 002 – 009 for ERCOT Asset Owners, Transmission & Distribution Owners, and Market Participants



# ERCOT Cyber Security Standards Workshop

Welcome and Kickoff

November 1, 2006

Jim Brenton, Director ERCOT Security  
ERCOT Cyber Security Rep to NERC CIPC

ERCOT - Public

# Antitrust Admonition

---

ERCOT strictly prohibits Market Participants and their employees who are participating in ERCOT activities from using their participation in ERCOT activities as a forum for engaging in practices or communications that violate the antitrust laws.

The ERCOT Board has approved guidelines for members of ERCOT Committees, subcommittees and working groups to be reviewed and followed by each Market Participant attending ERCOT meetings. If you have not received a copy of these Guidelines, please take one now and review it at this time. Please remember your ongoing obligation to comply with all applicable laws, including the antitrust laws.

- Welcome to ERCOT
- Safety and Evacuation Routes
- Introductions
- So, "How Did We Get to Here," and "What Should We Do Next?"
- ERCOT Workshop Goals and Objectives
- Preview Today's Agenda
- Breaks and Lunch Period

# Welcome to ERCOT

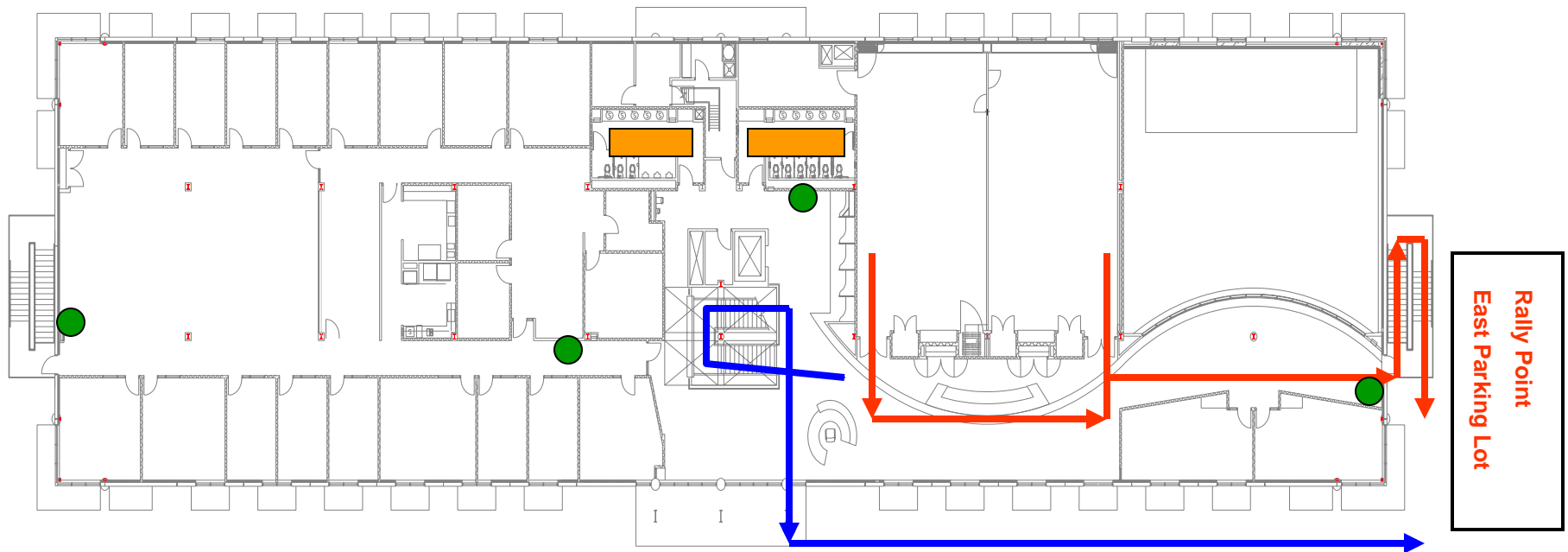
---

- Wireless and Wired Internet access available on Guest Network—Red Net
  - UserID and Password needed for Wireless
  - Use at your own risk—No special Security or Privacy measures in effect
- Electronic version of materials will be posted on [www.ercot.com](http://www.ercot.com) next week
- Breaks at approx 10am and 2pm
- Lunch at 11:40am
- Finish at 4pm

# Safety & Evacuation Routes

## Austin Facility

### Board Room / Prefunction



Red – Primary Exit Route

Blue – Secondary Exit Route

Safe Area – 1<sup>st</sup> floor

Fire Extinguisher

# Introductions

- **Cyber Security Standards Team Members Present**
  - Drafting Team
  - Education Team
- **Today's Guest Presenters**
  - Dyonyx: Ron Blume, Bill Addington, Jim Fortune
  - Burns & McConnell: Ben Church
  - KEMA: Jay Abshier
  - LCRA: Mike Allgeier
- **ERCOT Presenters**
  - Mark Henry—Compliance
  - Bill Bojorquez—Transmission Planning, CIPC Representative
  - Jeff Maddox—Information System Security
  - Jim Brenton—Cyber Security CIPC Representative
- **Other ERCOT Staff Members and Guests**
- **Each Participant – Please introduce your self**
  - Name and Company
  - What's your Role to implement NERC Cyber Security Std

# How Did We Get to Here?

- After 9/11, Urgent Action 1200 resulted in CIP 002-016 in CY-2003 which applied to the following NERC Entities
  - Balancing Authorities
  - Reliability Coordinators
  - Transmission Operators
- UA1300 resulted in four Draft versions of CIP 002-009 which were finally approved in May 2006 for June 2006 implementation
  - UA1200 NO Longer Exists and is NOT in effect
- CIP 002-009 submitted to FERC in Aug 2006 as ERO Standards
  - FERC has yet to act on CIP 002-009
  - CIP standards were not part of the 83 approved in October
  - FERC may conduct separate Public Rulemaking for CIP 002-009
  - Next FERC meeting scheduled for Nov 06—stay tuned



# What Should We Do Next?

- CIP 002-009 are NERC-approved industry Cyber Security Standards and they are in effect for NERC members
  - NERC recommends that all entities start implementation now
  - Registered NERC Entities are now subject to compliance audits, investigations, and sanctions for non compliance
  - Scope of Cyber Security standards has greatly expanded from Control Centers to now include other locations and assets
- NERC Cyber Security Workshops spent a full day on “What” the standards say and half a day on what “Compliance” documentation will be required during future compliance audits
- Today’s ERCOT Workshop today will
  - Focus on “How to get started” toward understanding the new standards and what does it take to get ready for compliance
  - Examine the “GAP” between what Standards require and where you are today
- This workshop is NOT A SUBSTITUTE for the NERC workshop
- We will NOT COVER the same material that NERC presents
  - If you have not attended, then REGISTER TODAY for one of the remaining NERC workshops

# Workshop Goals and Objectives

- Develop an awareness of
  - Current ERO and RRO activity
  - Need to perform GAP Analysis between your current state and what is required by new Cyber Security Stds: policies, processes, systems and technology
- Learn
  - What will ERCOT System Operations designate as ERCOT Critical Assets with respect to the Texas Bulk Power Grid
  - How Electronic and Physical Security Perimeters apply to Asset Owners and Transmission & Distribution Entities
  - Lessons from others implementing new Cyber Security Standards
- Technical Discussion of Critical Asset determination
- Understand that Compliance will NOT be something limited to just your IT or Security manager
  - How to gain Senior Executive support and action needed for Enterprise-wide Compliance with new standards
  - Include: HR, Legal, Contracting, CFO, Market Ops, System Ops

# CIP 002 Is the Key to Your Success

- First Identify all Critical Assets
- Then Identify Critical Cyber Assets
- Must use a Risk-Based Methodology (RBM)
- How to develop and apply a RBM? Go To: <http://www.esisac.com/library-assessments.htm>
  - Electric Sector Information Sharing and Analysis Center
  - Lists a number of risk-based methodologies
  - Select the one that best fits your needs
  - There will be other RBMs presented today

# Disclaimer and Final Thoughts

- The industry presenters here today are experienced service providers in the Electricity Sector who understand NERC Cyber Security Standards and have developed security solutions
  - All have been involved in standards drafting and implementation activities within our industry
  - The products and services presented are not “ERCOT-approved”
  - ERCOT cannot endorse or recommend any of these firms to best address your needs and requirements
  - There are other firms who offer similar skills, knowledge and abilities—you should perform due diligence to select the vendor that best meets your organization’s needs and requirements
  
- ERCOT greatly appreciates the time and effort that our industry presenters have contributed toward making this workshop a success—educational, informative, and productive. **THANK YOU in ADVANCE**
  
- **PLEASE**
  - Place all Cell Phones to silent or stun
  - Use the microphones for all questions and discussion
  - Take private or side conversations outside the room
  - Parking lot for off-topic items that we need to later address

# Agenda & Breaks

8:00 – 8:30	<b>Greeting and Introductions</b> Jim Brenton, Director of Security, ERCOT
8:30 – 9:00	<b>Regional Reliability Organization (RRO) Update</b> Mark Henry, Manager NERC Compliance, ERCOT
9:00 – 9:30	<b>ERCOT Critical Asset Criteria</b> Bill Bojorquez, Director of Transmission Services, ERCOT
9:30 – 10:10	<b>NERC CIP: How to Get Started – Gap Analysis</b> Ron Blume, Dyonyx
10:10 – 10:20	<b>10 Min Break</b>
10:20 – 11:00	<b>Cyber Security &amp; Substations: Defining Electronic Security Perimeter</b> Bill Addington, Dyonyx
11:00 – 11:40	<b>CIP: Do you know where your Critical Cyber Assets are?</b> Benjamin Church, Senior Manager, Burns & McConnell
11:40 – 12:40	<b>LUNCH Break</b>
12:40 – 1:20	<b>CIP: Risk-based Methods for Selecting Critical Assets</b> Benjamin Church, Senior Manager, Burns & McConnell
1:20 – 2:00	<b>Cyber Security Assessments – Lessons Learned</b> Jay Abshier, Senior Principal Consultant, KEMA
2:00 – 2:15	<b>10 Min Break</b>
2:15 – 3:30	<b>Panel Discussion: CIP 002: Just Exactly what is a “Critical Asset”?</b> Panel Chair: Bill Bojorquez, Director of Transmission Services, ERCOT • Mike Allgeier, Data Security Officer, LCRA • Jeff Maddox, Network Security Architect, ERCOT • Benjamin Church, Senior Manager, Burns & McDonnell • Jay Abshier, KEMA • Jim Fortune, Dyonyx
3:30 – 3:55	<b>Executive Call to Implementation</b> Jim Brenton, Director of Security, ERCOT
3:45 – 4:00	<b>Closing Remarks and Next Steps</b> Jim Brenton, Director of Security, ERCOT



Questions?