

Beyond Compliance

SANS SCADA Conference

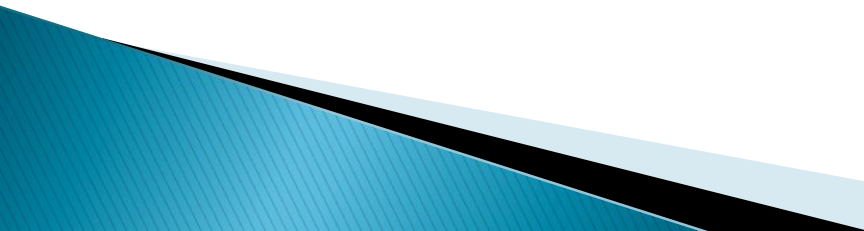
March 1, 2011

Jim Brenton

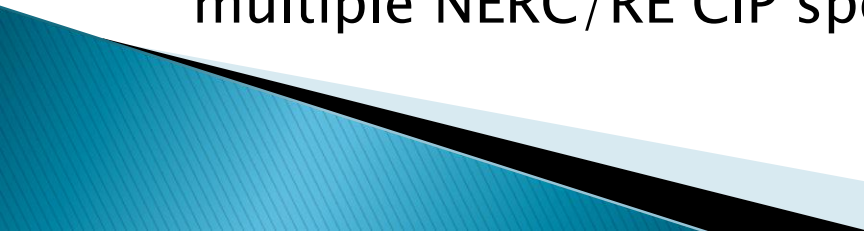
Regional Security Coordinator

ERCOT—Electric Reliability Council of Texas

ERCOT Disclaimer and Hold Harmless

- ▶ Facts expressed in this presentation are Facts
 - ▶ Opinions express in this presentation are solely my own
 - The voices I hear speak only to me
 - ▶ ERCOT should not be held accountable for my opinions and random ramblings
 - ▶ This presentation has NOT been reviewed by ERCOT Staff and does NOT represent ERCOT ISO or ERCOT Market Participant positions on any topic or issue that may be discussed
- 

Who/What is ERCOT?

- ▶ Electric Reliability Council of Texas—ERCOT
 - ▶ Independent System Operator (ISO) for Texas
 - Wholesale Generation and Retail Markets
 - Regulated by Texas Public Utility Commission
 - ▶ Texas Interconnection
 - ▶ Registered NERC functions include
 - Reliability Coordinator
 - Balancing Authority
 - Transmission Operator
 - Regional Transmission Planner
 - ▶ We have been fully CIP Compliant since July 2008 with multiple NERC/RE CIP spot checks and audits
- 


Compliance and Security Risks

- ▶ Security of the North American Bulk Electric System (BES) is too important to be left to voluntary industry participation
- ▶ Implementation of Cyber Security controls in the CIP Standards requires a different model than that of other BES Reliability Standards
 - Use of the BES Reliability Standards drafting and compliance models may actually reduce the overall security of the BES
 - Full NERC CIP Compliance does NOT mean that an Entity is fully Secure against Advanced Threat Actors in Contested Network Space

Compliance and Security Risks

- ▶ The Electricity Sector lacks a sufficient number of qualified security SMEs at all levels needed to properly implement Security
 - SecOps analysts; Audit, Compliance and Enforcement staff; and senior Executives and Boards of Directors
 - Training and Certification of security SMEs is a weak link
- ▶ Industry has placed far too much focus on compliance documentation and way too little attention on real-time security operations and monitoring
 - Just like FISMA—see OMB report on GAO and Agencies...


Hot Topics—*No Particular Order*

- ▶ Monitor Cyber Security Legislation and Executive Orders for new requirements
 - ▶ Track and Comment on emerging NERC CIP Standards—V4/V5 and CIP-010 & CIP-011
 - Involve key SME staff in Standards Development
 - ▶ NERC is moving to enhanced use of the ROP (Rules of Procedures), CANs (Compliance Application Notices), and RSAWS (Reliability Standards Auditor Worksheets) to implement security measures outside scope of the Reliability Standards Development Process (RSDP)
- 

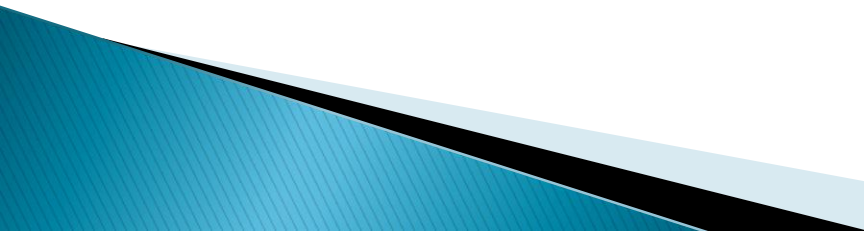
More Hot Topics—*Continued*

- ▶ Support Smart Grid
 - NERC/NIST/DoE Initiative to implement Smart Grid Guidelines based on the Smart Grid NISTR
 - Engage Smart Meter Vendors and Researchers
 - Privacy of Customer Information in AMI

 - ▶ Plan for SynchroPhasers Deployment
 - Network Architecture for Phasor Mgt Units
 - Be smart about CA/non-CA identification of SynchroPhaser components?

 - ▶ LMP (Local Marginal Pricing) and Nodal Market Models
- 

More Hot Topics—*Continued*

- ▶ Increased emphasis on timely application of Patches for known vulnerabilities
 - ▶ Enhanced Change Control and Configuration Management processes beyond CIP
 - ▶ Improve Vendor Contracts and Supply Chain Management to rapidly address remediation of emerging security vulnerabilities
- 

More Hot Topics—*Continued*

- ▶ Increase Real-Time Security Ops monitoring of networks and systems
 - Move from monitoring the external security perimeters required by CIP to comprehensive monitoring all internal and external transactions
 - Deep dive into event records and log files
 - Coordinate results and enhance information sharing with other industry entities
- ▶ Improve Public-Private Information Sharing with DoE/DHS
 - You need a Security Clearance through DHS

More Hot Topics—*Continued*

- ▶ Dept of Energy and the National Labs
 - INL and National SCADA Test Bed
 - PNNL and their Surveillance and Monitoring tools
- ▶ Department of Homeland Security and Local Protective Security Agents (PSA)
- ▶ Pre-coordinate with Local LEAs and your FBI office
- ▶ Security Event and Information Monitoring is key to successful Security Program
 - Do something with the log files required by NERC CIP Stds.
 - Deep dive and find out what is really happening on your networks

More Hot Topics—*Continued*

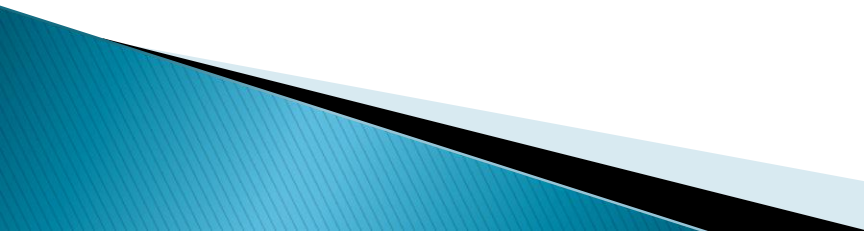
- ▶ Bottom Line: Move industry efforts away from “Audits, Compliance Documentation and Enforcements” of that of real security for CAs/BES to one based on continuous security performance monitoring of all networks and systems by qualified Security Ops Analysts and SMEs
- ▶ Set the Tone and Tenor from TOP of the Company
 - Engage Senior level Executives, Boards of Directors and State/Local Regulators in the CIP/Cyber Security Program

More Hot Topics—*Continued*

- ▶ Improve NERC Security Event Reporting
 - NERC Electric Sector ISAC reporting should NOT be the same as CIP - 008 Incident Report
 - EnergySec/EPRI—DoE/NESCO is the new kid on block

- ▶ Joint collaborative effort between NERC ES-ISAC and DoE/NESCO for betterment of industry outside of compliance functions

New Directions for NERC CIP Standards

- ▶ NERC/FERC need to move away from “Strict Compliance” of the current language in the CIP standards
 - Documentation violations should NOT result in significant fines or sanctions
 - ▶ CIP and Cyber Security are too important to be locked up in the FERC regulatory process
 - Too many lawyers making technical security decisions focused on strict compliance with Government Regulation
 - ▶ Change focus from managing “Compliance Risk” to that of managing “Security Risks”
- 

New Directions for NERC and CIP Stds

- ▶ Restructure CIP Standards to uniquely address security for Generation, Transmission & Distribution, Load Serving and Control Center Entities
 - One size does not fit all
 - Sound Security Controls for a Control Center could adversely affect reliability of Gen/Trans systems
- ▶ NERC members must step up and implement real security measures and controls for all environments
 - CA Identification of BES components is NOT the right issue
 - Better Secure all BES systems, AND other mission-critical systems and enterprise network systems and components
 - Congress and the public do NOT differentiate between BES, Market and Enterprise Systems

Avoid the “Abilene Paradox”

- ▶ The Abilene paradox is a situations in which a group of people collectively decide on a course of action that is counter to the preferences of any of the individuals in the group
- ▶ Current NERC Standards Development Process demonstrates the well-known pitfalls of this form of Dysfunctional Group Dynamics
 - How did we get to where we are today with CIP Standards?
 - Is anyone happy with where the Electricity Sector is today with respect to CIP and Cyber Security Controls? Industry, NERC/FERC, or Government?
 - What do we do to avoid repeating the same mistakes again?

Questions and Discussion