



ERCOT Cyber Security Standards Workshop

Executive Challenges for Cyber Security Implementation

November 1, 2006

Jim Brenton, Director of Security, ERCOT
Cyber Security Representative to NERC CIPC

ERCOT - Public

- **Compliance has become increasingly more important.**
 - Not just for the Cyber Security CIP Standards but for all system reliability areas.
 - EPAct of 2005



Energy Policy Act of 2005



- Heightened accountability for system reliability
- FERC oversight of all reliability standards and ENFORCEMENT where none existed before
- NERC role now as “strong” Electric Reliability Organization-ERO
 - Previously an Industry Organization
- NERC will now “drive and enforce” approved reliability standards that were previously “voluntary” standards

Energy Policy Act of 2005 continued ..

- Role of NERC Regional Entities expanding to include enforcement authority that will be “standardized” nationwide consistent with Regional Delegation Agreements
- Electric Sector Entities at all levels must now become “auditably compliant” with NERC standards or face possibility of monetary penalties



Who is Responsible for NERC Compliance?

- Electric Sector Entities must be Auditably compliant with
 - NERC Reliability Requirements, these include
 - Cyber Security Standards CIP 002 – CIP 009
- Cyber Security CIP standard compliance will require coordinated support from:
 - HR, Legal, Contracting, Project Management and Operations, plus other groups
 - Effort cannot be limited to just IT and Security groups



November 1, 2006



ERCOT - Public



More
↓

Most important:

- Every group that supports any aspect of compliance must attain an appropriate level of Cyber Security understanding consistent with their level of involvement supporting the NERC compliance process



Cyber Security Compliance Program Goals



- Develop a Cyber Security compliance program that is focused on continuous performance improvement
- Meet all Cyber Security compliance requirements through well-documented, auditable processes
- Properly maintain the content and protected storage of information needed to demonstrate Cyber Security compliance.
- Align organization and internal processes in a manner that fosters a compliance-focused culture

Regulation and Compliance Function

- CIP 003 requires that a senior manager be formally identified as the person responsible for the entity's adherence to CIP 002 – CIP 009 across all organizational functional areas
- Senior Manager or Executive responsibilities should include:
 - Monitor Cyber Security compliance and oversight for all areas
 - Ensure written policies, standards and operating procedures that document and track to NERC Cyber Security Standards
 - Maintenance of a NERC Cyber Security Standards database to ensure company-wide tracking and support

- Establish clear Cyber Security compliance roles and responsibilities across all Organizational functions
- Ensure that all staff members are Educated and Trained on the Cyber Security Compliance process
- Monitor and Coordinate the status and pending actions with each Cyber Security Requirement Owner in the company
- Communicate current Cyber Security Standard status for all functional departments to Corporate Executives



Cyber Security Requirement Owners

- Identify Requirement Owners for each Cyber Security Standard
- Each Requirement Owner must be accountable for the implementation of Cyber Security processes within their areas of responsibility
 - Educate and train all staff members on compliance with Cyber Security Standard requirements
 - Perform a Gap Analysis and identify any missing Policies, Procedures, Processes and Technologies needed for compliance with Cyber Security Standards
 - Perform Risk Assessment for each item found during the Gap Analysis

Requirement Owners continued..

- Consult with qualified Subject Matter Experts on how to best close Gaps and mitigate known Cyber Security Risks
- Develop and execute plans to close Gaps and mitigate risks
- Report status and actions to the Manager or Executive responsible for the Regulation and Compliance function

Reliability and Risk Management Function

- Designate a Senior Manager or Executive with experience in Reliability and Risk functions with the responsibility to:
 - Conduct and lead independent, internal risk assessment audits of Cyber Security functions
 - Identify opportunities for Cyber Security process improvement
 - Identify compliance issues and Recommend corrective action plans



- Track and ensure that corrective action plans are implemented to reduce Risk
- Report Cyber Security readiness status and recommendations the Executives responsible for Cyber Security compliance functions
- Independently Report Risk Mitigation actions and Cyber Security status to the CEO and Corporate Executives



Steps for Cyber Security Success



- **Set the “Tone at the Top”**— Corporate Officers and Executives
- Make sure that CEO is aware of expanded scope of Cyber Security CIP Standards → May need to Engage
 - Board of Directors
 - PUCT or other Regulatory Bodies
- Establish an Executive Officer Oversight or Steering Committee
 - Brief Executive Committee as Key Stakeholders
 - Conduct one-on-one meetings with all officers as needed for support

Steps continued..

- Assign senior Program Manager to oversee Cyber Security Implementation
 - Corporate Officers must have a High Level of confidence in this person
 - Coordinate the efforts of individual project teams
 - Ensure appropriate Security milestones in SDLC process
- Develop Functional Teams to identify Critical Assets and Cyber Assets
 - Each Officer must assign team members to ensure commitment
- Hold an Official Kickoff Meetings for each Functional Project
 - Obtain participation and demonstrate support from Corporate Officers
 - Ensure all members support the Project and understand overall Cyber Security Program Goals
 - Deliver lists of Critical Assets and Critical Cyber Assets



Steps continued..

- Perform Gap Analysis of all Corporate Policies, Standards, Procedures, Processes and Technologies against the new Cyber Security Standards
 - Key step for success—Pick the right SMEs
 - Engage a vendor with experience in this skill
- Develop new Policies, Standards and Procedures to reflect new Processes and Technologies implemented to support new Cyber Security Standards
 - Documentation must meet NERC Compliance expectations
 - See NERC Compliance Presentation
 - Processes and Technology must be aligned with Corporate standards *and* goals
 - Documentation must be used and updated – not allowed to become “shelfware” for auditors



Steps continued..

- Highly experienced Program Managers must
 - Require new projects and technologies to meet NERC Cyber Security Standards
 - Ensure ongoing operations and maintenance of existing systems must continue
 - Monitor existing resources that may become overwhelmed
 - Add staff or augment with contractor support as needed
- Clearly communicate to all that previous NERC “self assessments” of UA1200 will now be “Compliance Audits” with potential monetary impact
 - First Audits could happened in Summer 2007 with FERC/NERC emphasis on audit results
 - Implementation schedule Increases Compliance Standards each year
 - Bad press for non-compliance will be an factor
 - FERC/NERC monetary fines and PUCT action may occur for compliance audit failures



Example Cyber Security Planning Milestones

1. Formally designate a Senior Manager or Executive for CIP Cyber Security
2. Establish an Executive Officer Oversight or Steering Committee
3. Assign Program Manager
4. Perform GAP Analysis and Develop Preliminary Risk Management Plans
5. Develop Functional Project Teams to address specific project tasks
6. Develop and Gain approval for new documentation and Obtain Project Funding for New Technology and Systems to meet new Cyber Security Standards
7. Transition projects from planning to execution and production status

- Formally designate a Senior Manager or Executive for CIP Cyber Security
 - Responsible for adherence to CIP Standards 002 – CIP 009 across all organizational functional areas
- Establish an Executive Officer Oversight or Steering Committee
 - Brief Management Committee as Key Stakeholders
 - Conduct one-on-one meetings with all officers
- Assign Program Manager
 - Corporate Officers must have a High Level of confidence in this person
 - Coordinate the efforts of individual project teams

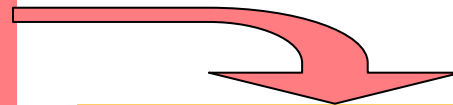
Example Planning Milestones in detail..

- Identify CIP Sponsors and CIP Asset Owners
- Develop Functional Project Teams to address specific project tasks
 - Each Officer must assign team members to ensure commitment

Form Critical Asset Identification Team
—Hold Kickoff Meeting

Develop Risk-Based Methodology to
Identify Critical Assets

Finalize Critical Asset List



Form Critical Cyber Asset Identification Team
—Hold Kickoff Meeting

Develop Preliminary Critical Cyber Asset List

Finalize Critical Cyber Asset List

- Perform GAP Analysis and Develop Preliminary Risk Management Plans
- Develop and Gain approval for new documentation and Obtain Project Funding for New Technology and Systems to meet new Cyber Security Standards
- Transition projects from planning to execution and production status
 - Train and prepare future system owners to operate and maintain documentation for audits



Successful Governance is Critical

- Top-Down verse Bottom-Up approach
- MUST HAVE Executive Management Buy-in & Stakeholder Support
 - Executive Sponsor for each new project
 - VP/Executive Oversight or Steering Team
 - Establish supporting Workgroups for technical details
 - Dedicated Program Manager to shepherd various Compliance Projects thru PMO to completion



Successful Governance continued..



- Director/Management-level team members designated as process owners
- Senior Risk Manager or Reliability Compliance Officer in charge of monitoring/audit of Cyber Security program
- Strong links to Corporate Board of Directors
 - Finance and Audit Committee—Internal Controls Management Process and Internal Audit
 - Governance and HR—Personnel Risk Assessment, On-boarding and Exiting employees/contractors

Critical Decision Points Needed for Success

- Strong controls and process needed:
 - Formally designate a senior manager to be responsible for the entity's Cyber Security Compliance
 - Designation of "critical assets" for company
 - Also Coordinate if you have ERCOT-designated CAs
 - Designation of "critical cyber assets" to support CAs
 - Assignment of Program Manager
 - Selection of external consultants as needed
 - Selection of a methodology for risk-based assessments process
 - Designation of Risk Manager or Reliability Compliance Officer that independently reports to CEO and Executives
 - Rigorous sign-off process at all phases



Risk Assessment are Key to Success

- Vulnerability and Risk Assessments
 - Conduct strong GAP analysis
 - Carefully select an experienced consultant that is respected in the industry
 - Develop strong documentation on internal and/or external risk assessments conducted on each Cyber Security CIP requirement
 - Strive to do more than the minimum needed to minimize corporate risk of NERC/FERC audit exceptions



Risk Assessment continued..

- Take off the blinders that may have been used during UA1200 Self Assessments
 - Don't just see what you want to see
 - Ensure that everything is documented with artifacts and evidence of well-functioning program, not just paper compliance



Summary

- Need a strong corporate commitment to build a successful compliance program
- Need an aggressive but achievable timeline
- Develop a strong governance model
- Institute effective critical decision approval process
- Do multiple level detailed assessments and gap analysis
- Obtain Management Sign-off at each step is critical
- Develop action plans aligned with CIP implementation dates that management will support

Questions and Discussion



Thank You !