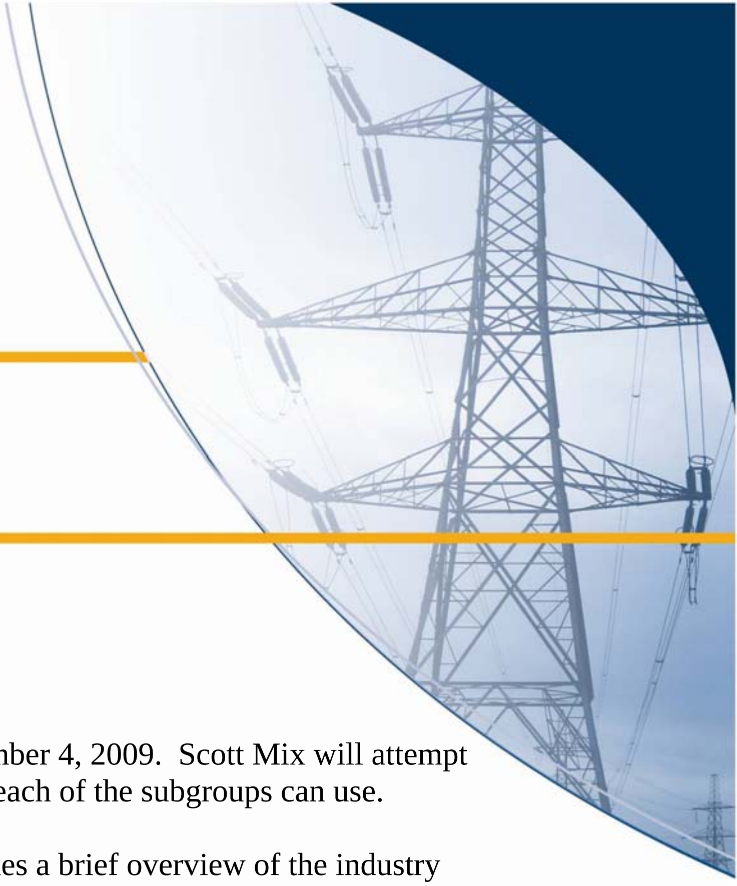
NERC

NORTH AMERICAN ELECTRIC
RELIABILITY CORPORATION



Meeting Notes
CS706SDT Leadership Team

September 1, 2009

Coordination with Subgroup Leaders

Comments on the Concept paper are due by September 4, 2009. Scott Mix will attempt to put the comments together quickly in ways that each of the subgroups can use.

The proposed meeting agenda for next week includes a brief overview of the industry comments up front, and if the subgroups have had a chance to review the comments in advance, they can offer any initial reflections as part of their initial progress report. The agenda includes 45 minutes for each subgroup report on day one. The subgroups will review these inputs when they break out in the afternoon of day one and the morning of day 2.

Subgroup Leaders Roll Call:

- Scott Mix
- Kevin Perry
- Joe Bucciero
- Hal Beardal
- Phil Huff
- John Lim
- Joe Doetzl
- Jay Cribb
- Jim Breton

1. Reliability Functions Subgroup Update and Coordination Issues — Jim Breton (for John Varnell)

The Subgroup is meeting Thursday morning and trying to set up a meeting with Jackie Collett's BES Subsystems and BES Cyber systems subgroup on Thursday at 11:00 a.m. CST to talk about transition. How to turn our work over to that group is the key. What would this look like in terms of applicability and how to evaluate which functions do you perform?

Participant Comments

- This gets more complex as we move forward. One server can be on four components with different high or low values.

- Everything will have security on it. It will be a huge job to evaluate everything.

2. **List of BES Subsystems and BES Cyber systems Subgroup Update and Coordination Issues — Jay Cribb (for Jackie Collett)**
The team was unaware of the Functions subgroup trying to set up a joint meeting. They have base requirements but need reliability functions to complete their task. The concept paper is very loose regarding lists. There is a remaining concern about possibly requiring compliance on every nut and bolt on the system.

Participant Comments

- Documentation for compliance taking time away from and attention to security? Focus on high and medium for audits and not audit low unless there is an event that must be documented.
- Acknowledge that that is the NIST model and the Rockefeller/Snowe Bill.
- Lot of work but industry will probably vote it down
- The current politics, waiting for a negative vote. What is the alternative?
- Cannot demonstrate everything on every system. I would love for the SDT to step through the process on each system from start to finish. No one has gone through to make sure it will work.
- Other participants thought this was a good idea
- Internally within the SDT? Yes
- Get requirements first then walk through demonstration.
- Need to make the whole process as simple as possible and limit discretionary decision making. What do I need to do to be in compliance?
- Looking at systems impacting reliability
- What are we auditing against?
- Review with Jeri, Keith and others in terms of how NIST works now
- Should be looking at compliance not management
- Take a look at risk based methodology now

3. **BES Mapping Subgroup Update and Coordination Issues — John Lim**
The team is scheduled to meet this Wednesday to clean up the document. If we have performance based criteria will not applicable to all cases. What if thresholds don’t work?

For generation, transmission, etc. looking to group in related systems. They will need a full list of functions

4. **Cyber Analysis Subgroup Update and Coordination Issues — Phil Huff**
The Subgroup is working to determine the final categorizations to present next week. The team is not sure they have the experts they need to finish the list. Even if you have all the BES functions, what does high mean in certain power generation situations? The team may need more input from John or Jackie’s teams. Detailed thresholds would be a serious bottleneck. Jay’s suggestion is that the SDT needs to walk through examples to illustrate application and

identify implications make sense. Perhaps in California the team could go through some real life examples.

Participant Comments

- We will need to understand how evaluation will be applied and implications. Apply to digital pressure gauge on a steam line?

Definition and Selection of Controls Subgroup Update and Coordination Issues — Keith Stouffer

Kevin Perry reported that there have been no meetings of Keith's group since Charlotte.

Summary and Next Steps

- Each group will review with others key issues in reports on day one
- Small group work will follow that
- Thursday morning small groups can look at and work on the "seams"
- Possibly end with a concept outline to integrate drafts on Thursday afternoon
- Can we work out guidelines?
- Auditors can only audit to standards/requirements, not to guidelines. Auditors assess compliance.
- Phil, Scott and Kevin (with other minor contributions) got into discussing an example to illustrate possible application of high/medium/low categorization on a BES – low production transformer. Assess function, not the asset? Asset may serve different functions
- Jay Cribb ended the conversation by noting this was a good discussion and illustrated why they need to walk through example(s) as a full group