~~Security-Related Information – Withhold Under 10 CFR 2.390~~ ABW

DIABLO CANYON POWER PLANT
PROCESS PROTECTION SYSTEM REPLACEMENT
NSIR Meeting June 7, 2011

George Hough
Pacific Gas and Electric
GDH2@pge.com
805-545-4291

Scott B. Patterson
Pacific Gas & Electric Co.
sbp1@pge.com
805-545-4082

Ken Schrader
Pacific Gas & Electric Co.
kjse@pge.com
805-545-4328

John Hefler
Altran Solutions Corp.
jhefler@altransolutions.com
415-543-6111

Ted Quinn
Altran Solutions Corp.
tedquinn@cox.net
415-543-6111

Greg Clarkson
Altran Solutions Corp.
gretg@rockcreektech.com
415-543-6111

NSIR Meeting Agenda (1000 to 1200)

- Introductions
- Diablo Canyon Power Plant (DCPP) Cyber Security Program Schedule
- Process Protection System (PPS) Replacement Schedule
- NSIR update on inspection acceptance criteria for meeting RG 5.71
- Programmatic approach to Cyber Security for PPS
- Cyber Security requirements for the PPS
  - Vendor requirements
  - PG&E requirements
- Summary
- Discussion

DCPP Cyber Security – Implementation Schedule

- Cyber Security Plan Submitted -- April 4, 2011 [redacted]
  - Proposed Implementation Schedule
  - NRC is Reviewing
- Prioritized Implementation Schedule
  - Critical Milestones – December 31, 2012
  - Full Implementation – Plant Specific
  - Dates viewed as commitments by the NRC

DCPP Process Protection System Replacement – Implementation Schedule

- Two vendors
  - Westinghouse/CS Innovations
    - Topical Report submitted and being reviewed
    - Will not be approved before LAR Submittal
    - Per ISG-06 the Westinghouse/CSI scope will be Tier 3
  - Invensys/Triconex
    - Topical Report submitted and being reviewed
    - Will be approved before LAR Submittal
    - Per ISG-06 the IOM/Triconex scope will be Tier 1
- LAR Submittal – July 2011 (30 days after Triconex v10 Topical Report is approved)
- LAR Approval – March 2013 (~20 months after submittal)
- Unit 1 Installation – February 2014
- Unit 2 Installation – October 2014

NSIR update on inspection acceptance criteria for meeting RG 5.71

- To be provided by NRC NSIR

DCPP Cyber Security Program

- Programmatic Approach
  - [redacted]
- Critical Digital Asset (CDA) Determination
- CDA Multilayered Defense
  - [redacted]
  - [redacted]
- Full CS Involvement in CDA Life Cycle
- Periodic Program Review

DCPP Cyber Security – Vendor Support

[redacted]

[redacted]

- Vendor compliance is a contract issue

- Certification Process Needed

DCPP Cyber Security – PPS

- CS Involved in all project phases

- Full Protection for PPS
  - Physical Protections
  - Network Protections
  - Operation and Maintenance Procedures

DCPP Cyber Security – Summary

- CS Program Implementation in progress
  - Some Milestones Complete
  - Budgets Allocated
  - Senior management support
- DCPP Involved with Industry
  - NEI, INPO, STARS, USA,
- DCPP Connected to National CS Support [redacted]

Cyber Security Requirements

- Includes
  - Vendor requirements
  - PG&E requirements

Cyber Security Requirements

- Vendor Requirements:
  - [redacted]
  - What is the expectation for vendors with respect to providing assurance of a secure development and operating environment?
    - Some vendors will not release specific information
    - Legacy software/firmware – How to address?
    - Operating Systems

Cyber Security Requirements for PPS

- PG&E Requirements
  - [redacted]
- PPS Requirements
  - [redacted]

Summary

- PG&E committed to cyber security compliance in accordance with the DCPP Cyber Security Plan.
- PPS will be evaluated to the same acceptance criteria applicable to all systems for cyber security.