

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.
kise@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 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

ABW

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

ABW

ABU

DCPP Cyber Security – Vendor Support

[REDACTED]

[REDACTED]

[REDACTED]

□ Vendor compliance is a contract issue

■ Certification Process Needed

ABU

ABW

DCPP Cyber Security – PPS

- CS Involved in all project phases



- Full Protection for PPS

- Physical Protections
- Network Protections
- Operation and Maintenance Procedures

ABW

ABW

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



ABW

APW

Cyber Security Requirements

- Includes
 - Vendor requirements
 - PG&E requirements

APW

Cyber Security Requirements

■ Vendor Requirements:



- 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

BBW

Cyber Security Requirements for PPS

■ PG&E Requirements

- [Redacted]
- [Redacted]

■ PPS Requirements

- [Redacted]
- [Redacted]
- [Redacted]
- [Redacted]
- [Redacted]
- [Redacted]

BBW

Summary

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