From: Wang, Alan
Sent: Friday, March 04, 2011 8:37 AM
To: 'Baldwin, Thomas (DCPP)'; 'Soenen, Philippe R'
Cc: Lent, Susan; Burkhardt, Janet
Subject: Diablo Canyon Cyber Security Plan Request for Additional Information (ME4290 and ME4291)

Tom and Larry,

By letter dated July 22, 2010 (Agencywide Documents Access and Management System (ADAMS) Accession No. ML102150081), Pacific Gas and Electric Company (PG&E) submitted PG&E Letter DCL-10-087, "License Amendment Request 09-05, Request for Approval of the Diablo Canyon Power Plant Cyber Security Plan and Revision to the Facility Operating Licenses," which superseded the previous submittal on January 20, 2010. PG&E submitted a request for revision to the Facility Operating License Nos. DPR-80 and DPR-82 and review and approval of the Cyber Security Plan (CSP) for the Diablo Canyon Power Plant, Unit Nos. 1 and 2 (DCPP), in accordance with Title 10 of the *Code of Federal Regulations* (10 CFR), Section 73.54, "Protection of digital computer and communication systems and networks."

The U.S. Nuclear Regulatory Commission (NRC) staff has reviewed the information provided in your application and determined that the following additional information is required in order to complete its review. This request for additional information (RAI) was discussed with Mr. Larry Parker of your staff on March 2, 2011, and it was agreed that a response would be provided by April 4, 2011. If circumstances result in the need to revise the requested response date, please contact me at (301) 415-1445 or via e-mail at Alan.Wang@nrc.gov. The NRC staff has determined that no security-related or proprietary information is contained herein.

1. Records Retention

The regulations in 10 CFR 73.54(c)(2) requires licensees to design a cyber security program to ensure the capability to detect, respond to, and recover from cyber attacks. Furthermore, 10 CFR 73.54(e)(2)(i) requires licensees to maintain a CSP plan that describes how the licensee will maintain the capability for timely detection and response to cyber attacks. The ability for a licensee to detect and respond to cyber attacks requires accurate and complete records and is further supported by 10 CFR 73.54(h), which states that the licensee shall retain all records and supporting technical documentation required to satisfy the requirements of 10 CFR Section 73.54 as a record until the Commission terminates the license for which the records were developed, and shall maintain superseded portions of these records for at least 3 years after the record is superseded, unless otherwise specified by the Commission.

The licensee's CSP in Section 4.13 states that Critical Digital Asset (CDA) audit records and audit data (e.g., operating system logs, network device logs) are retained for a period of time that is less than what is required by 10 CFR 73.54(h).

Please explain the deviation from the 10 CFR 73.54(h) requirement to retain records and supporting technical documentation until the Commission terminates the license (or to maintain superseded portions of these records for at least 3 years) and how that meets the requirements of 10 CFR 73.54.

2. Implementation Schedule

The regulations in 10 CFR 73.54 require licensees to submit a CSP that satisfies the requirements of this section for Commission review and approval. Furthermore, each submittal must include a proposed implementation schedule and the implementation of the licensee's cyber security program must be consistent with the approved schedule. Paragraph 73.54(a) of 10 CFR requires licensees to provide high assurance that digital computer and communication systems and networks are adequately protected against cyber attacks, up to and including the design basis threat.

The completion of several key intermediate milestones (items (a) through (g) below) would demonstrate progress toward meeting the requirements of 10 CFR 73.54. The NRC staff's expectation is that the key intermediate milestones will be completed in a timely manner, but no later than December 31, 2012. The key CSP implementation milestones are as follows:

a) Establish, train and qualify Cyber Security Assessment Team, as described in Section 3.1.2, "Cyber Security Assessment Team," of the CSP.

b) Identify Critical Systems and CDAs, as described in Section 3.1.3, "Identification of Critical Digital Assets," of the CSP.

c) Implement cyber security defense-in-depth architecture by installation of [deterministic one-way] devices, as described in Section 4.3, "Defense-In-Depth Protective Strategies," of the CSP.

d) Implement the management, operational and technical cyber security controls that address attacks promulgated by use of portable media, portable devices, and portable equipment as described in Appendix D, Section 1.19, "Access Control for Portable and Mobile Devices," of Nuclear Energy Institute (NEI) 08-09, Revision 6.

e) Implement observation and identification of obvious cyber related tampering to existing insider mitigation rounds as described in Appendix E, Section 4.3, "Personnel Performing Maintenance and Testing Activities," and Appendix E, Section 10.3, "Baseline Configuration," of NEI 08-09, Revision 6.

f) Identify, document, and implement cyber security controls to physical security target set CDAs in accordance with Section 3.1.6, "Mitigation of Vulnerabilities and Application of Cyber Security Controls," of the CSP.

g) Ongoing monitoring and assessment activities will commence for those target set CDAs whose security controls have been implemented, as described in Section 4.4, "Ongoing Monitoring and Assessment," of the CSP.

h) Full implementation of the CSP for all safety, security, and emergency preparedness functions.

Please provide a revised CSP implementation schedule that identifies the appropriate milestones, completion dates, supporting rationale, and level of detail to allow the NRC

to evaluate the licensee's proposed schedule and associated milestone dates which include the final completion date. It is the NRC's intention to develop a license condition incorporating your revised CSP implementation schedule containing the key milestone dates.

3. Scope of Systems

Paragraph 73.54(a) of 10 CFR requires licensees to provide high assurance that digital computer and communication systems and networks are adequately protected against cyber attacks, up to and including the design basis threat as described in 10 CFR 73.1. In addition, 10 CFR 73.54(a)(1) states that

> The licensee shall protect digital computer and communication systems and networks associated with:
>
> (i) Safety-related and important-to-safety functions;
>
> (ii) Security functions;
>
> (iii) Emergency preparedness functions, including offsite communications; and
>
> (iv) Support systems and equipment which, if compromised, would adversely impact safety, security, or emergency preparedness functions.

Subsequent to the issuance of the cyber security rule, the NRC stated that 10 CFR 73.54 should be interpreted to include structures, systems, and components (SSCs) in the balance of plant (BOP) that have a nexus to radiological health and safety (ADAMS Accession No. ML103490344, dated November 19, 2010). The SSCs in the BOP are those that could directly or indirectly affect reactivity of a nuclear power plant and could result in an unplanned reactor shutdown or transient and are, therefore, within the scope of important-to-safety functions described in 10 CFR 73.54(a)(1). Furthermore, the NRC issued a letter to NEI dated January 5, 2011 (ADAMS Accession No. ML103550480) that provided licensees with additional guidance on one acceptable approach to comply with the Commission's policy determination.

Please explain how the scoping of systems provided by CSP for DCPP, meets the requirements of 10 CFR 73.54 and the additional guidance provided by the NRC.