UNITED STATES
NUCLEAR REGULATORY COMMISSION
REGION IV
1600 EAST LAMAR BOULEVARD
ARLINGTON, TEXAS 76011-4511

January 8, 2020

Mr. James M. Welsch
Senior Vice President, Generation
and Chief Nuclear Officer
Pacific Gas and Electric Company
P.O. Box 56
Mail Code 104/6
Avila Beach, CA 93424

SUBJECT: DIABLO CANYON POWER PLANT, UNITS 1 AND 2 - NOTIFICATION OF CYBER SECURITY INSPECTION (NRC INSPECTION REPORT 05000275/2020401 AND 05000323/2020401) AND REQUEST FOR INFORMATION

Dear Mr. Welsch:

On April 27, 2020, the U.S. Nuclear Regulatory Commission (NRC) will begin an inspection in accordance with Inspection Procedure (IP) 71130.10P, "Cyber Security," Revision 0, at Diablo Canyon Power Plant, Units 1 and 2. This inspection evaluates and verifies your ability to meet the full implementation requirements of the NRC's Cyber Security Rule, Title 10, *Code of Federal Regulations* (CFR), Part 73, Section 54, "Protection of Digital Computer and Communication Systems and Networks." The onsite portion of the inspection will take place during the weeks of April 27 and May 11, 2020.

Experience has shown that these inspections are extremely resource intensive, both for the NRC inspectors and licensee staff. In order to minimize the inspection impact on the site and to ensure a productive inspection for both parties, we have enclosed a request for documents needed for the inspection. The document request has been divided into four groups.

The first group specifies information necessary to assist the team in choosing the focus areas (i.e., "sample set") to be inspected in accordance with the cyber security inspection procedure. This information should be made available using either a secure document management service or passive media (i.e. CD, DVD) and delivered to the regional office no later than March 9, 2020. The inspection team will review this information and by the end of the planned information gathering visit on April 10, 2020, will request the specific items that should be provided for review.

The second group of requested documents will assist the team in their evaluation of the critical systems and critical digital assets, defensive architecture, and the areas of the cyber security plan selected for inspection. This information will be requested for our review in the regional office prior to the inspection, by April 20, 2020.

The third group of requested documents consists of those items that the team will review or need access to, during the inspection. Please have this information available by the first day of the onsite inspection, April 27, 2020.

The fourth group of information is necessary to aid the team in tracking issues identified as a result of the inspection. It is requested that this information be provided to the lead inspector as the information is generated during the inspection. It is important that all of these documents are up to date and complete in order to minimize the number of additional documents requested during the preparation and/or the onsite portions of the inspection.

The lead inspector for this inspection is Sam Graves. We understand that our regulatory contact for this inspection is Amanda Sorensen and our technical contact is Chance Siri. If there are any questions about the inspection or the material requested, please contact the lead inspector at 817-200-1102 or by e-mail at Samuel.Graves@nrc.gov.

**PAPERWORK REDUCTION ACT STATEMENT**

This letter contains mandatory information collections that are subject to the Paperwork Reduction Act of 1995 (44 U.S.C. 3501 et seq.). The Office of Management and Budget (OMB) approved these information collections (approval number 3150-0011). Send comments regarding this information collection to the Information Services Branch, Office of the Chief Information Officer, Mail Stop: T6 A10M, U.S. Nuclear Regulatory Commission, Washington, DC 20555-0001, or by e-mail to Infocollects.Resource@nrc.gov, and to the Desk Officer, Office of Information and Regulatory Affairs, NEOB-10202, (3150-0011) Office of Management and Budget, Washington, DC 20503.

**Public Protection Notification**

The NRC may not conduct nor sponsor, and a person is not required to respond to, a request for information or an information collection requirement unless the requesting document displays a currently valid OMB control number.

This letter, its enclosure, and your response (if any) will be made available for public inspection and copying at http://www.nrc.gov/reading-rm/adams.html and at the NRC Public Document Room in accordance with 10 CFR 2.390, “Public Inspections, Exemptions, Requests for Withholding.”

Sincerely,

***/RA/***

Samuel T. Graves, Senior Reactor Inspector
Engineering Branch 2
Division of Reactor Safety

Docket Nos. 05000275 and 05000323
License Nos. DPR-80 and DPR-82

Enclosure:
Diablo Canyon Power Plant –
Cyber Security Inspection Document Request

cc w/encl: Electronic Distribution

DIABLO CANYON POWER PLANT, UNITS 1 AND 2 - NOTIFICATION OF CYBER SECURITY INSPECTION (NRC INSPECTION REPORT 05000275/2020401 AND 05000323/2020401) AND REQUEST FOR INFORMATION – JANUARY 8, 2020

**DISTRIBUTION:**
SMorris, ORA
MShaffer, ORA
TVegel, DRP
MHay, DRP
RLantz, DRS
GMiller, DRS
CNewport, DRP
JReynoso, DRP
JJosey, DRP
RAlexander, DRP
MArel, DRP
VDricks, ORA
BSingal, NRR
RAzua, DRS
PJayroe, DRS
BCorrell, DRS
MHerrera, DRMA
R4Enforcement
DCylkowski, ORA
JWeil, OWFN
AMoreno, OWFN
JQuichocho, OEDO
BMaier, ORA

ADAMS ACCESSION NUMBER: ML20009E890

| ☒ SUNSI Review: By: STG | ADAMS: ☒ Yes ☐ No | ☐ Non-Publicly Available ☒ Publicly Available | ☒ Non-Sensitive ☐ Sensitive | Keyword: NRC-002 |
|---|---|---|---|---|

| OFFICE | SRI:EB2 | | | | | |
|---|---|---|---|---|---|---|
| NAME | SGraves | | | | | |
| SIGNATURE | ***/RA/*** | | | | | |
| DATE | ***1/8/2020*** | | | | | |

**OFFICIAL RECORD COPY**

**Diablo Canyon Power Plant – Cyber Security Inspection Document Request**

| | |
|---|---|
| **Inspection Report:** | 05000275/2020401 and 05000323/2020401 |
| **Inspection Dates:** | Weeks of April 27 and May 11, 2020 |
| **Inspection Procedure:** | IP 71130.10P, "Cyber Security," Revision 0 |
| **Reference 1:** | ML17156A215 - "Guidance Document for Development of the Request for Information (RFI) and Notification Letter for Full-Implementation of the Cyber Security Inspection," Revision 1, dated October 26, 2017 |


| | | |
|---|---|---|
| **NRC Inspectors:** | Sam Graves, Lead<br>817-200-1102<br>Samuel.Graves@nrc.gov | Shiattin Makor<br>817-200-1507<br>Shiattin.Makor@nrc.gov |
| **NRC Contractors:** | Casey Priester<br>301-415-7000<br>Frederick.Priester@nrc.gov | Leyton Pitzer<br>301-287-0582<br>Leyton.Pitzer@nrc.gov |


## *I. Information Requested for In-Office Preparation*

The initial request for information (i.e., first RFI) provides the team with the general information necessary to select appropriate components and cyber security plan elements to develop a site-specific inspection plan. The team will use the first set of information requested to identify the list of critical systems and critical digital assets plus operational and management security control portions of the cyber security plan to be chosen as the "sample set" required to be inspected during this inspection. The first information request is specified in Table RFI #1. Provide the first set of information to the team lead in the regional office, by March 9, 2020, or sooner, to facilitate the selection of the specific items that will be reviewed during the onsite inspection weeks.

The requested information shall be provided on either a secure document management service or passive media (i.e. CD or DVD) to the lead inspector. If passive media is chosen, please provide four copies of each media submitted (i.e., one for each inspector/contractor). The preferred file format for all lists is a searchable Excel spreadsheet file on a CD or DVD. These files should be indexed and hyperlinked to facilitate efficient review. If you have any questions regarding this information, please contact the inspection team lead as soon as possible.

| Table RFI #1 | | |
|---|---|---|
| **Section 3: Initial Documentation Requests (See Reference 1) Paragraph Number/Title:** | | **Items** |
| 1 | List all identified critical systems and critical digital assets | All |
| 2 | List critical digital asset facility and site ethernet – transmission control protocol/internet protocol (TCP/IP) based local area networks (LANs) and identify those LAN's that have non-critical digital assets on them | All |
| 3 | List critical digital asset facility and site non-ethernet TCP/IP based LANs including those industrial networks and identify LANs that have non-critical digital assets on them | All |
| 4 | Network topology diagrams (be sure to include all network intrusion detection systems and security information and event management (SIEMs) for emergency preparedness (EP) networks and security level 3 and 4 networks) | All |
| 8 | List all network security boundary devices for EP networks and all network security boundary devices for levels 3 and 4 | All |
| 9 | List critical digital asset wireless Industrial networks | All |
| 11 | Network Intrusion detection system documentation for critical systems that have critical digital assets associated with them | 11.a.1)<br>11.a.2) |
| 12 | SIEM documentation for critical systems that have critical digital assets associated with them | 12.a.1)<br>12.a.2) |
| 14 | List EP and security onsite and offsite digital communication systems | All |
| 25 | Cyber security assessment and cyber security incident response teams | All |
| 28 | Copy of current cyber security plan and copy of any 50.54(p) analysis to support changes to that plan | All |
| 29 | Copy of any licensee identified violations and associated corrective action program documentation to resolve issue(s) | All |

In addition to the above information please provide the following:

(1) Electronic copy of the updated safety analysis report and technical specifications
(2) Name(s) and phone number(s) for the regulatory and technical contacts
(3) Current management and engineering organizational charts related to cyber security
(4) Cyber security program procedures

Based on this information, the team will identify and select specific systems and equipment (e.g., critical systems and critical digital assets) from the information requested by Table RFI #1 and submit a list of specific systems and equipment to your staff by the end of the information gathering visit on April 10, 2020, for the second information request (i.e., Table RFI #2).

## *II. Additional Information Requested to be Available Prior to Inspection*

As stated in Section I, the team will examine the documents from the initial information request and submit the list of specific systems and equipment to your staff by the end of the information gathering visit. This second information request (i.e., Table RFI #2) obtains additional documents required to evaluate the critical systems and critical digital assets, defensive architecture, and the areas of the cyber security program selected for the cyber security inspection. The additional information requested for the specific systems and equipment is identified in Table RFI #2. All requested information shall follow the guidance document Reference 1.

The Table RFI #2 information shall be provided on a secure document management service or passive media to the lead inspector, by April 20, 2020, or sooner. Please provide four copies of each CD/DVD submitted (i.e., one for each inspector/contractor). The preferred file format for all lists is a searchable Excel spreadsheet file on a CD/DVD. These files should be indexed and hyperlinked to facilitate efficient review. If you have any questions regarding this information, please call the inspection team lead as soon as possible.

| Table RFI #2 | | |
|---|---|---|
| **Section 3: Initial Documentation Requests (See Reference 1) Paragraph Number/Title:** | | **Items** |
| 5 | Plant computer system block diagram (if plant computer system is selected for inspection) | All |
| 6 | Plant security system block diagram (if security computer system is selected for inspection) | All |
| 7 | Block diagrams for distributed systems (for systems selected for inspection) | All |
| 10 | Host-based intrusion detection system documentation for critical digital assets (for systems selected for inspection) | 10.a.1)<br>10.a.2) |
| 13 | List all maintenance and test equipment (M&TE) used on critical digital assets (for systems selected for inspection) | All |
| 15 | Configuration management | All |
| 16 | Supply chain management | 16.a<br>16.b |
| 17 | Portable media and mobile device control | All |
| 18 | Software management | All |
| 20 | Vendor access and monitoring | All |
| 21 | Work control | All |
| 22 | Device access and key control | All |
| 23 | Password/authenticator policy | All |

| Table RFI #2 | | |
|---|---|---|
| **Section 3: Initial Documentation Requests (See Reference 1) Paragraph Number/Title:** | | **Items** |
| 24 | User account/credential policy | All |
| 26 | Corrective actions since last NRC inspection | All |
| 27 | Cyber security assessments for selected systems | All |

In addition to the above information please provide the following:

(1) Names and positions of the CSAT and CSIRT members.

(2) Copies of lesson plans and training presented to the CSAT and CSIRT members, continuing technical training for engineers, as well as any general awareness training.

(3) List of dates of CSAT meetings that have occurred.

## *III. Information Requested to be Available on First Day of Inspection*

For the specific systems and equipment identified in Section II, provide the following request for information (i.e., Table 1st Week Onsite) on a secure document management service or passive media, by April 27, 2020, the first day of the inspection. All requested information shall follow the guidance in Reference 1.

Please provide four copies of each CD submitted (i.e., one for each inspector/contactor). The preferred file format for all lists is a searchable Excel spreadsheet file on a CD/DVD. These files should be indexed and hyperlinked to facilitate ease of use. If you have any questions regarding this information, please call the inspection team lead as soon as possible.

| Table 1st Week Onsite | | |
|---|---|---|
| **Section 3: Initial Documentation Requests (See Reference 1) Paragraph Number/Title:** | | **Items** |
| 10 | Host-based intrusion detection system documentation for critical digital assets (for systems selected for inspection) | 10.a.3) thru 10.a.12) |
| 11 | Network Intrusion detection system documentation for critical systems that have critical digital assets associated with them | 11.a.3) thru 11.a.15) |
| 12 | SIEM documentation for critical systems that have critical digital assets associated with them | 12.a.3) thru 12.a.14) |
| 16 | Supply chain management | 16.c |
| 19 | Cyber security event notifications | All |

| Table 1st Week Onsite | | |
|---|---|---|
| **Section 3: Initial Documentation Requests (See Reference 1) Paragraph Number/Title:** | | **Items** |
| 29 | Update to licensee identified violations and corrective action program actions taken since the initial request was made | All |

In addition to the above information please provide the following:

(1) Copies of the following documents do not need to be solely available to the inspection team as long as the inspectors have easy and unrestrained access to them.

a. Quality Assurance Plan;

b. Technical Specifications, if not previously provided;

c. Latest Individual Plant Examination/Probabilistic Risk Assessment Report; and,

(2) Vendor Manuals, Assessments, and Corrective Actions:

a. The most recent cyber security quality assurance audit and/or self-assessment; and

b. Corrective action documents (e.g., condition reports, including status of corrective actions) generated as a result of the most recent cyber security quality assurance audit and/or self-assessment.

***IV: Information Requested To Be Provided Throughout the Inspection***

(1) Copies of any corrective action documents generated as a result of the inspection team's questions or queries during the inspection.

(2) Copies of the list of questions submitted by the inspection team members and the status/resolution of the information requested (provided daily during the inspection to each inspection team member).

If you have any questions regarding the information requested, please contact the team lead.