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

November 20, 2012

Mr. Peter Dietrich
Senior Vice President and
Chief Nuclear Officer
Southern California Edison Company
San Onofre Nuclear Generating Station
P.O. Box 128
San Clemente, CA 92674-0128

SUBJECT: SAN ONOFRE NUCLEAR GENERATING STATION - NOTIFICATION TO PERFORM INSPECTION OF TEMPORARY INSTRUCTION 2201/004, "INSPECTION OF IMPLEMENTATION OF INTERIM CYBER SECURITY MILESTONES 1-7," AND REQUEST FOR INFORMATION (05000361/2013405, 05000362/2013405)

Dear Mr. Dietrich:

On February 25, 2013, the U.S. Nuclear Regulatory Commission (NRC) will begin an inspection of Southern California Edison Company's cyber security program (CSP) implementation for San Onofre Nuclear Generating Station, Units 2 and 3, using the guidance in Temporary Instruction 2201/004, "Inspection of Implementation of Interim Cyber Security Milestones 1-7." The inspection will be performed to assess and verify your ability to meet the interim milestone 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."

In accordance with 10 CFR 73.54, each nuclear power plant licensee was required to submit a proposed cyber security plan and implementation schedule for NRC approval. On December 14, 2009, by letter (ML093080517) to the Nuclear Energy Institute (NEI), the NRC provided their expectations for the proposed implementation schedule. On January 5, 2011, by letter (ML110060093) to the NRC, NEI issued an initial "Template for the Cyber Security Plan Implementation Schedule" (ML110060097). On February 28, 2011, by letter (ML110600206) to the NRC, NEI provided a revised, "Template for the Cyber Security Plan Implementation Schedule." The purpose of the letter's attachment was to provide licensees with a generically written template to develop their proposed CSP implementation schedule. Utilization of the generic template required the licensee to make conforming changes to ensure the submitted schedule accurately accounted for site-specific activities. Based on an NRC technical review (ML110070348), the template was found acceptable to develop the licensees' CSP implementation schedule (i.e., Milestones 1 through 8).

On July 22, 2010, as supplemented by letters, dated September 29, 2010, November 30, 2010, and March 31, 2011, Southern California Edison submitted a cyber security plan for the San Onofre Nuclear Generating Station, Units 2 and 3, following the template in NEI 08-09, Revision 6, "Cyber Security Plan for Nuclear Power Reactors," dated April 2010. On March 31, 2011, Southern California Edison supplemented their cyber security plan to address scope of systems in response to the October 21, 2010, Commission decision, records retention issues, and implementation schedule concerns (ML11112A028). The NRC staff considers the March 31, 2011, supplement as the approved schedule as required by 10 CFR 73.54.

The inspection of the interim cyber security program at San Onofre Nuclear Generating Station, Units 2 and 3, will be limited to the verification of implementation of Milestones 1 through 7. Temporary Instruction 2201/004, "Inspection of Implementation of Interim Cyber Security Milestones 1-7" provides a programmatic level review and verification of the site-specific implementation of these milestones.

The schedule for the onsite inspection for Milestones 1 through 7 is as follows:

- Information Gathering Visit: February 12 – 14, 2013
- Milestone Inspection: February 25 – March 1, 2013

The purpose of the information gathering visit is to: (1) obtain information and documentation needed to support the TI inspection; (2) become familiar with the San Onofre Nuclear Generating Station Cyber Security Program, personnel, and plant layout; and (3) arrange logistical details, such as office space, availability of knowledgeable staff, and to ensure unescorted site access privileges.

In order to assure an efficient inspection, we have enclosed a request for information describing documents needed to aid the inspectors in preparing for and conducting the temporary instruction inspection. These documents have been divided into four groups. The first group lists information necessary to aid the inspectors in planning for the TI inspection. It is requested that this information be provided to the lead inspector via mail or electronically no later than January 22, 2013. The second group also lists information and possible areas for discussion necessary to assist the inspectors during the TI inspection. It is requested this information be available during the information gathering visit (February 12 – 14, 2013). The third group of requested documents consists of those items that the inspectors will review, or need access to, during the TI inspection. Please have this information available by the first day of the onsite inspection week (February 25, 2013). The fourth group lists the information necessary to aid the inspectors in tracking questions and answers identified as a result of the TI inspection. It is requested that this information be provided to the lead inspector as the information is generated during the TI 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 TI inspection.

The lead inspector is Sam Graves. We understand that our contact for this inspection is Ryan Pettus. If there are any questions about the inspection or the material requested, please contact the lead inspector at (817) 200-1102, or via e-mail at samuel.graves@nrc.gov.

This letter does not contain new or amended information collection requirements subject to the Paperwork Reduction Act of 1995 (44 U.S.C. 3501 et seq.). Existing information collection requirements were approved by the Office of Management and Budget, control number 3150-0011. The NRC may not conduct or 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 Office of Management and Budget control number.

In accordance with 10 CFR 2.390 of the NRC's "Rules of Practice," a copy of this letter and its enclosure will be available electronically for public inspection in the NRC Public Document Room or from the Publicly Available Records (PARS) component of NRC's document system (ADAMS). ADAMS is accessible from the NRC Web site at http://www.nrc.gov/reading-rm/adams.html (the Public Electronic Reading Room).

Sincerely,

/RA/

Geoffrey Miller, Chief
Engineering Branch 2
Division of Reactor Safety

Dockets: 50-361; 50-362
Licenses: NPF-10; NPF-15

Enclosure:
Cyber Security Temporary Instruction (TI) 2201/004 (Milestones 1 – 7)
Request for Information

Electronic Distribution to San Onofre

Electronic distribution by RIV:
Regional Administrator (Elmo.Collins@nrc.gov)
Deputy Regional Administrator (Art.Howell@nrc.gov)
DRP Director (Kriss.Kennedy@nrc.gov)
Acting DRP Deputy Director (Barry.Westreich@nrc.gov)
Acting DRS Director (Tom.Blount@nrc.gov)
Acting DRS Deputy Director (Jeff.Clark@nrc.gov)
Senior Resident Inspector (Greg.Warnick@nrc.gov)
Resident Inspector (John.Reynoso@nrc.gov)
Administrative Assistant (Heather.Hutchinson@nrc.gov)
Branch Chief, DRP/D (Ryan.Lantz@nrc.gov)
Senior Project Engineer (Nick.Taylor@nrc.gov)
Project Engineer, DRP/D (Brian.Parks@nrc.gov)
Public Affairs Officer (Victor.Dricks@nrc.gov)
Public Affairs Officer (Lara.Uselding@nrc.gov)
Project Manager (Randy.Hall@nrc.gov)
Branch Chief, DRS/TSB (Ray.Kellar@nrc.gov)
RITS Coordinator (Marisa.Herrera@nrc.gov)
Regional Counsel (Karla.Fuller@nrc.gov)
Technical Support Assistant (Loretta.Williams@nrc.gov)
Congressional Affairs Officer (Jenny.Weil@nrc.gov)
OEMail Resource
RIV/ETA: OEDO (Cayetano.Santos@nrc.gov)
DRS/TSB STA (Dale.Powers@nrc.gov)

R:\ ADAMS ML12325A914

ADAMS: □ No ☒ Yes	☒ SUNSI Review Complete	Reviewer Initials: GBM
	☒ Publicly Available	☒ Non-Sensitive
	□ Non-publicly Available	□ Sensitive

SRI::DRS/EB2	C: DRP/PBD		C:DRS/EB2
STGraves	RELantz		GBMiller
11/19/12	11/20/12		11/20/12
/RA/	/RA/		/RA/

OFFICIAL RECORD COPY T=Telephone E=E-mail F=Fax

CYBER SECURITY TEMPORARY INSTRUCTION (TI) 2201/004 (MILESTONES 1 – 7)
REQUEST FOR INFORMATION

Inspection Report: 05000361/2013405, 05000362/2013405

Onsite Dates: February 12 – February 14, 2013 (Information Gathering Visit)
February 25 – March 1, 2013 (Cyber Security TI Inspection)

Procedure: Temporary Instruction 2201/004, "Inspection of Implementation of Interim Cyber Security Milestones 1 – 7"

NRC Inspectors: Samuel Graves, Lead Inspector
(817) 200-1102
samuel.graves@nrc.gov

Nestor Makris
(817) 200-1384
nestor.makris@nrc.gov

Security Contractor, To Be Determined

I. Information Requested Prior to the Information Gathering Visit

The following information is requested by **January 22, 2013**. Electronic media is preferred. Where information is provided that includes tables and/or lists of data or other such information, please do not scan such tables and/or lists as images. The preferred file format is a searchable portable document format (pdf) file on transportable media (CD/DVD). The information should be indexed and hyperlinked to facilitate use. Please provide three copies of each CD submitted (one for each inspector and for a cyber security contractor).

A. Cyber Security TI Documentation

1. Please provide a list of all documents necessary to support verification of the TI requirements for each of the Cyber Security Milestones (1 through 7) identified in Enclosure 3 - SONGS Cyber Security Plan Proposed Implementation Schedule. Identify and describe each milestone in a separate folder on the media (e.g., Milestone 1, Milestone 2, etc.). If the milestone description differs from those described in the Temporary Instruction, provide a cross-reference between them. Provide each milestone in a separate folder on the media (e.g., Milestone 1, Milestone 2, etc.). Each milestone document shall be listed in a table as follows:

MILESTONE X (where X equals 1 through 7)				
Document Number	Title	Description	Revision	Status
No. 1				
No. 2				
No. 3				
etc				

Based on the list of documents identified in **I.** A.1 above, for each milestone document where the "Status" is identified as completed, place the completed document in its associated folder and hyperlink the associated document number to the completed document. For each document, the "Status" should be identified as "not started," "in-progress" or "completed."

Please ensure the documents identified in **I.**A.1 above include the documents identified below (**I.**A.2 - **I.**A.8) for **MILESTONES 1 - 7** and are included in the **I.**A.1 table.

2. **MILESTONE 1 –** Provide the following documentation for the Cyber Security Assessment Team (CSAT):

   a. Procedures establishing the CSAT team.

   b. List of CSAT members noting primary areas of responsibility.

   c. Procedures detailing qualification requirements for CSAT members.

   d. Supporting documentation that demonstrates each CSAT member meets the requirements to fulfill their respective position on the team. For example, member resumes; evaluation of previous education and experience; training required by your implementing procedures and supporting documentation which shows training was completed; or industry certifications).

3. **MILESTONE 2** – Provide the following documentation:

   a. List of plant systems noting which systems have been identified as critical systems (CSs).

   b. Procedure documenting the process by which CSs and Critical Digital Assets (CDAs) are identified in accordance with your CSP.

4. **MILESTONE 3** – Provide the following documentation:

   a. Procedures establishing your cyber defensive architecture. Explain any variances from your CSP and tracking documents for their correction.

   b. Provide an overview of your cyber defensive architecture, preferably with overview level diagrams showing the various levels and location of the subject deterministic one-way device.

   c. Provide details of the implementation of the subject deterministic one-way device.

5. **MILESTONE 4** – Provide the following documentation:

   Procedures implementing the security control "Access Control for Portable and Mobile Devices." Include any training material or promotional literature distributed to staff associated with the control.

6. **MILESTONE 5** – Provide the following documentation:

   a. Procedures implementing the requirements described in Milestone 5.

b. Training materials associated with the changes to plant programs associated with Milestone 5

7. **MILESTONE 6** – Provide the following documentation:

   Procedures documenting the process by which technical cyber security controls have been identified for those CDAs which require the implementation of technical security controls for Milestone 6.

8. **MILESTONE 7** – Provide the following documentation:

   Procedures implementing the ongoing monitoring and assessment activities as described in your CSP.

B. Cyber Security Supporting Documentation

1. Provide a copy of the current version of the updated safety analysis report (USAR), Technical Specifications (TS), and technical requirements manual (TRM) or equivalent.
2. Provide a copy of the current cyber security "Health Report," if available.
3. Provide a copy of the current plant drawings used for operator training that provide additional information on system operation, system operating parameters, setpoints, etc. (e.g., some licensee's refer to these drawings as "Horse Notes") for identified cyber security CSs, if available.
4. Provide operator training lesson plans and/or operator training aids for identified cyber security CSs, if available.

II. Information Requested During the Information Gathering Visit (February 12 – 14, 2013)

The following information is requested to be provided to the inspectors during the onsite information gathering visit. It is requested that the following information be provided on three sets of searchable CD/DVDs.

A. General Information:

1. A listing of abbreviations and/or designators for plant systems;
2. Organizational chart for corporate and site personnel involved in establishing, overseeing, and maintaining the Cyber Security Program and;
3. A phone list for licensee personnel.

B. Facility Information:

1. Provide a presentation/discussion of your CSP, existing cyber security CSs, and associated CDAs.

2. Provide a list and discussion of currently scheduled or planned cyber security related modifications to be installed in the plant.

C. Specific Information Associated with the Milestones:

1. Provide a presentation/discussion of your CSP, existing cyber security CSs, and associated CDAs.

2. **MILESTONE 3** - Be prepared to provide an overview walkdown of the cyber architecture within the plant including safety, security and emergency preparedness related CDAs.

3. **MILESTONE 6** - Be prepared to present information for target set CDAs including a list of target set CDAs, and documentation of the process for identifying them.

4. **MILESTONE 6 -** For selected CDAs, be prepared to provide documentation for **each** of the technical controls in Appendix D of NEI 08-09, Revision 6, the results of reviews required under your CSP.

   (a) For controls that are implemented, provide the procedures implementing the control. Common controls for all CDAs may be provided in a separate list with the procedures implementing each of them.

   (b) For alternate controls that have been implemented, provide the documented basis for employing alternative countermeasures, and the procedures implementing the alternative measures.

   (c) Where controls have been deemed unnecessary, provide the threat vector analysis supporting the conclusion that the threat vector does not exist.

5. **MILESTONE 7 -** For the CDAs selected above, be prepared to provide documentation for **each** of the technical controls in Appendix D of NEI 08-09, Revision 6, and the results of immediate activities required under your CSP.

   (a) For all controls that are implemented, provide the objective evidence that the control is effective IAW your CSP. This may be combined with the documentation provided for Milestone 6.

   (b) Documentation for common controls for all CDAs may be provided in a separate list with the procedures implementing each of them.

   (c) Provide governing procedures and results of vulnerability scans performed to comply with your CSP.

III. Information Requested to be Available on First Day of the Onsite Inspection Week (February 25, 2013)

Any updates to information previously provided.

IV. Information Requested to be Provided Throughout the Temporary Instruction Inspection Assessment

Copies of the list of questions/documents requested identified by the inspector and the status/resolution of the information requested (provided daily during the TI inspection to each inspector).

If you have questions regarding the information requested, please contact the lead inspector, Sam Graves, (817) 200-1102, or by email to samuel.graves@nrc.gov.