SOUTHERN CALIFORNIA EDISON®
An EDISON INTERNATIONAL® Company

Thomas J. Palmisano
Vice President Decommissioning &
Chief Nuclear Officer

10 CFR 50.90

September 6, 2016

U. S. Nuclear Regulatory Commission
ATTN: Document Control Desk
Washington, D.C. 20555

Subject: **Docket No. 50-361 and 50-362**
Supplement 1 to Amendment Applications 271 and 256
Proposed Changes to Cyber Security Plan
Implementation Schedule Completion Date
San Onofre Nuclear Generating Station, Units 2 and 3

References: (1) Letter from T. J. Palmisano (SCE) to Document Control Desk (NRC) dated June 16, 2016; Subject: Docket No. 50-361 and 50-362, Amendment Applications 271 and 256, Proposed Changes to Cyber Security Plan Implementation Schedule Completion Date, San Onofre Nuclear Generating Station, Units 2 and 3 (ADAMS Accession No. ML16172A075)

(2) Memorandum from R. Felts (NRC) to B. Westreich (NRC), "Review Criteria for Title 10 of the Code of Federal Regulations Part 73.54, Cyber Security Implementation Schedule Milestone 8 License Amendment Requests," dated October 24, 2013 (ADAMS Accession No. ML13295A467).

Dear Sir or Madam:

By letter dated June 16, 2016 (Reference 1), Southern California Edison (SCE) submitted license amendment applications 271 and 256 to operating licenses NPF-10 and NPF-15 for San Onofre Nuclear Generating Station (SONGS) Units 2 and 3, respectively. The proposed amendments requested a change to the Cyber Security Plan Implementation Schedule Milestone 8 completion date.

Following discussions with the NRC, SCE has evaluated the proposed amendments using the guidance provided in an NRC memorandum dated October 24, 2013 (Reference 2). The Enclosure to this letter provides Supplement 1 to Reference 1 by evaluating SCE's proposed changes using the eight criteria described in Reference 2.

SCE has determined that this Supplement does not affect the conclusions of the No Significant Hazards Consideration or the Environmental Consideration of the proposed change provided in Reference 1.

SDO1A
NRR

P.O. Box 128
San Clemente, CA 92674
(949) 368-6575
Fax: (949) 368-6183
tom.palmisano@sce.com

There are no new regulatory commitments in this letter or the Enclosure.

Should you have any questions, or require additional information, please contact Mr. Jim Kay at (949) 368-7418.

I declare under penalty of perjury that the foregoing is true and correct.

Executed on 09/06/2016

Sincerely,

JAMES A MADIGAN
FOR TJP

Enclosures:
Supplement 1 to Amendment Applications 271 and 256

cc: K. Kennedy, Regional Administrator, NRC Region IV
M. Vaaler, NRC Project Manager, SONGS Units 1, 2 and 3
S. Y. Hsu, California Department of Public Health, Radiologic Health Branch

ENCLOSURE

Supplement 1 to Amendment Applications 271 and 256

For SONGS Units 2 and 3

By letter dated June 16, 2016, Southern California Edison (SCE) submitted license amendment applications 271 and 256 to operating licenses NPF-10 and NPF-15 for San Onofre Nuclear Generating Station (SONGS) Units 2 and 3, respectively. The proposed amendments requested a change to the Cyber Security Plan Implementation Schedule Milestone 8 completion date.

An NRC memorandum provides eight criteria for the review of license amendment requests to revise the schedule for the Implementation Milestone 8 completion date. The following technical evaluation provides information concerning the eight criteria that explains the current status of the SONGS cyber security program and the need for the Implementation Milestone 8 completion date revision. The evaluation describes how prioritization of both the SONGS completed and planned implementation actions will provide assurance that digital computer and communication systems and networks are adequately protected against cyber attacks up to and including the design basis threat established by 10 CFR 73.1(a)(1)(v).

3.2.1 Identification of the Specific Requirements of the Cyber Security Plan that SCE needs Additional Time to Implement (Criterion 1)

SCE is requesting a two year extension to the due date for implementation of the following requirement of the Cyber Security Plan (Milestone 8):

Cyber Security Plan, Section 3.1, "Analyzing Digital Computer Systems and Networks and Applying Cyber Security Controls":

- Mitigation activities

3.2.2 Detailed Justification that Describes the Reason SCE Requires Additional Time to Implement the Specific Requirements (Criterion 2)

The purpose of the SONGS Cyber Security Plan is to provide protection against cyber-attacks for CDAs in Structures, Systems, and Components (SSCs) that provide a significant Safety, Security, or Emergency Preparedness (SSEP) function at Units 2 and 3 and the Independent Spent Fuel Storage Installation (ISFSI). Following transition to an ISFSI-only configuration, Critical Systems (CS) that performed SSEP functions at Units 2 and 3 will no longer be required and, consequently, the current CDAs associated with those functions will no longer be protected subject to 10 CFR 73.54.

The SONGS decommissioning plan supports moving the spent fuel from the spent fuel pool to the ISFSI by the end of 2019 (with a potential early finish date of mid-2018) at which time implemented system mitigations associated with SSEP functions at Units 2 and 3 (i.e., a majority of mitigations) will be removed from service. As the decommissioning agent, SONGS

believes that resources allocated to mitigation of CDAs that will shortly be removed from service is not a prudent use of resources. *The proposed extension would allow SCE to forego mitigation of those CDAs that would no longer be required in an ISFSI-only configuration, as the associated SSEP functions would be eliminated by transition to an ISFSI-only configuration prior to the time that the mitigations are required to be completed.*

3.2.3 A Proposed Completion Date for Milestone 8 Consistent with the Remaining Scope of the Work to be Continued and Resources Available (Criterion 3)

SONGS is requesting a change to the Implementation Milestone 8 completion date from December 31, 2017 to December 31, 2019.

3.2.4 An Evaluation of the Impact that Additional Time to Implement the Requirements will have on the Effectiveness of the SCE Overall Cyber Security Program in the Context of Milestones Already Completed (Criterion 4)

Based on the cyber security implementation activities completed to date, and the ongoing cyber security project activities, SONGS is already cyber secure and will continue to ensure that digital computer and communication systems and networks are adequately protected against cyber-attacks.

SONGS successfully completed the implementation of the interim Implementation Milestones 1 through 7 by December 31, 2012, as approved by the NRC and described in License Condition 2.E. The implementation of these milestones provides a high degree of protection against cyber-attacks. The completed activities include:

- Implementation Milestone 1: Establish Cyber Security Assessment Team (CSAT)
  - Cyber Security Program procedure and CDA assessment procedure establishing the CSAT is issued
  - CSAT in place, training developed and delivered

- Implementation Milestone 2: Identify Critical Systems (CSs) and CDAs
  - An engineering document for identifying CSs and CDAs was issued
  - CSs and CDAs have been identified and documented
  - CDA defensive levels were determined and documented using the SONGS Cyber Security Defensive Strategy. SONGS has identified five (5) defensive levels in the cyber security defensive architecture

- Implementation Milestone 3: Implement cyber security defense-in-depth architecture including deterministic boundary isolation devices (i.e., diodes)
  - Installed boundary isolation devices (diodes) to deterministically eliminate bi-directional communication pathways between Security Level 4 to Security Level 3 and between Security Level 3 to Security Level 2
    - Security Level 4 to Security Level 3 communication pathways boundary isolation device
      - A boundary isolation device (diode) was installed, as part of milestone 3, for the Plant Computer System Application (R*time) User Datagram Protocol (UDP) data stream from the Plant Computer System (PCS) network in the plant (Level 4) outbound only to the receive side of the diode providing communications to

Security Level 3 [This connection was removed from service in 2015 during the elimination of the Emergency Operations Facility]
    - Security Level 3 to Security Level 2 communication pathways boundary isolation devices
        - A boundary isolation device (diode) was installed, as part of milestone 3, for Plant Computer System R*time UDP data stream from the PCS network (Security Level 3) outbound only to the receive side of the diode providing communications to Security Level 2 [This connection was removed from service in 2015 during the elimination of the Emergency Operations Facility]
        - Provides a UDP data stream from the Gamma Spectroscopy System (Security Level 3) network outbound only to the receive side of the diode providing communications to Security Level 2
  - A connectivity analysis was completed to verify no unauthorized communication pathways or bypasses are present

- Implementation Milestone 4: Implement Portable Media and Mobile Device (PMD) Control Program
  - Portable media scanning is accomplished through the implementation of scanning kiosks
    - Kiosks are stand-alone isolated scanning stations with no network connectivity. Updates are performed via an approved manual process
    - Kiosks use eight scanning engines, six of which are heuristic
  - Mobile device scanning is accomplished through implementation of malware scanning tools
  - PMD scanning tools and scanning kiosks further minimize the threat from PMDs that connect to CDAs

- Implementation Milestone 5: Implement observation program for obvious cyber-related tampering
  - Training developed and delivered to Security personnel (subsequent to Milestone 5 completion, Operations personnel were also trained to observe for obvious cyber-related tampering)
  - Authorized individual roles and responsibilities established

- Implementation Milestone 6: Identify, document, and implement cyber security controls for CDAs within scope of physical security target set equipment
  - SONGS procedure SO23-IV-2.1, Revision 2, "Security Target Sets," requires the Target Set Expert Panel to meet on an annual basis. Additional meetings may be held at the request of any member of the Target Set Expert Panel. Additionally, target set review is required by the procedure to identify changes to plant configurations or modifications to systems and components, which require review by the Target Set Expert Panel. The Target Set Expert Panel met on July 17, 2013, to address changes to the plant because SONGS is no longer an operating plant. It was determined by the Expert Panel that SONGS no longer has physical security target set equipment that contains CDAs.

- Implementation Milestone 7: Ongoing monitoring and assessment activities for target set CDAs
  - The ongoing monitoring and assessment activities program for target set CDAs was implemented prior to the December 31, 2012 Milestone due date. The program, however, is no longer required as a result of the findings from the Target Set Expert Panel meeting on July 17, 2013.

- Implementation of Milestone 8 (Full Program Implementation) is in progress. Assessments for all remaining CDAs are underway and will be completed by the currently required date of December 31, 2017. The Program infrastructure integrating the Cyber Security procedures and training into the plant processes is underway and will be completed by the current Milestone 8 completion date of December 31, 2017 [ready for implementation, if needed]. The new spent fuel pool cooling system CDAs have been assessed and mitigated. Additionally, SONGS has fully implemented 10 CFR 73.77 Cyber Security Event Notification rule which provides the NRC with notification of cyber-attacks in order to inform the U.S. Department of Homeland Security (DHS) and federal intelligence and law enforcement agencies of cyber security-related events that could (1) endanger public health and safety or the common defense and security, (2) provide information for threat-assessment processes, or (3) generate public or media inquiries.

Based on the above measures to implement the Cyber Security Program milestones, the impact proposed extension to the Implementation of Milestone 8 on the effectiveness of the over-all cyber security program will be minimal.

3.2.5 A Description of the SCE Methodology for Prioritizing Completion of the Work for Critical Digital Assets Associated with Significant Safety, Security, or Emergency Preparedness Consequences and with Reactivity Effects in the Balance of Plant (Criterion 5)

SONGS has abandoned all Safety Related CDAs since SONGS is in a permanently shutdown and defueled condition. All spent fuel is expected to be in dry storage by the end of 2019 (with a potential early-finish date of mid-2018).

All remaining CDAs (including security CDAs) are being assessed. These assessments are currently scheduled to complete by the existing Milestone 8 date of December 31, 2017.

3.2.6 A Discussion of the SCE Cyber Security Program Performance up to the Date of the License Amendment Request (Criterion 6)

The Interim Implementation Milestones 1 through 7 activities completed by December 31, 2012 provide a high degree of protection against cyber security related attacks. These include:

- PMD Control Program
  - The overall implementation is effective. SONGS has addressed in the SONGS corrective action program (CAP), corrective actions pertaining to handling of media, industry lessons learned, issues with kiosks and scanning anomalies.

- Defense-in-Depth and Diodes (Security Level 4 to Security Level 3 and Security Level 3 to Security Level 2).
  - The integrity of the diodes is intact based on the implemented design.
  - Analysis has been completed to verify that no Security Level 4 to Security Level 3 two-way communication exists. Security Level 4 and Security Level 3 systems are presently deterministically isolated.

The NRC issued an inspection report of the SONGS Implementation of Milestones 1 through 7 on April 15, 2013, and no NRC-identified or self-revealing findings were identified during the inspection. While a single licensee-identified violation was listed in the inspection report, the

NRC determined the violation to be of very low security significance (i.e., Green as determined by the Physical Protection Significance Determination Process) and was treated as a non-cited violation. Inspection observations were entered into the SONGS CAP. An independent self-assessment of the program for Implementation Milestones 1 through 7 has been performed, and all identified findings and recommendations are either complete or being tracked to completion in the SONGS Corrective Action Program (CAP).

3.2.7 A Discussion of Cyber Security Issues Pending in the SCE Corrective Action Program (CAP) (Criterion 7)

SONGS uses the CAP to document cyber security issues to trend, correct, and improve the SONGS cyber security program. The CAP documents and tracks from initiation through closure, cyber security required actions including issues identified during on-going program assessment activities. Adverse trends are monitored for program improvement and addressed through the CAP process. Examples of resolved issues and activities pending in the CAP are:

- Pending activity - Full program (Implementation Milestone 8) implementation tracking
- Resolved activities include:
  - Industry and NRC lessons learned for SONGS cyber security program improvement
  - Issues and improvement items identified pertaining to the implemented portions of the cyber security program
  - Operating experience and pertinent threat release impact evaluations

3.2.8 A Discussion of Modifications Completed to Support the Cyber Security Program and a Discussion of Pending Cyber Security Modifications (Criterion 8)

Modifications completed to support the cyber security program:

- Implemented design change packages for installation of boundary isolation devices (diodes) to deterministically eliminate bi-directional communication pathways between Security Level 4 to Security Level 3 and between Security Level 3 to Security Level 2.

  - Security Level 4 to Security Level 3 communication pathways boundary isolation devices.
    - A boundary isolation device (diode) was installed, as part of milestone 3, for the Plant Computer System Application (R*time) User Datagram Protocol (UDP) data stream from the Plant Computer System (PCS) network in the plant (Level 4) outbound only to the receive side of the diode providing communications to Security Level 3 [This connection was decommissioned in 2015 during the elimination of the Emergency Operations Facility.]

  - Security Level 3 to Security Level 2 communication pathways boundary isolation devices.

- A boundary isolation device (diode) was installed, as part of milestone 3, for Plant Computer System R*time UDP data stream from the PCS network (Security Level 3) outbound only to the receive side of the diode providing communications to Security Level 2 [This connection was decommissioned in 2015 during the elimination of the Emergency Operations Facility]
- Provides a UDP data stream from the Gamma Spectroscopy System (Security Level 3) network outbound only to the receive side of the diode providing communications in Security Level 2.