UNITED STATES
NUCLEAR REGULATORY COMMISSION
WASHINGTON, D.C. 20555-0001

February 24, 2017

Mr. Thomas J. Palmisano
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, UNITS 2 AND 3 – CORRECTION LETTER FOR LICENSE AMENDMENT NOS. 234 AND 227 REGARDING REVISION OF THE CYBER SECURITY PLAN MILESTONE 8 COMPLETION DATE IN THE FACILITY OPERATING LICENSES (CAC NOS. L53132 AND L53133)

Dear Mr. Palmisano:

By letter dated January 23, 2017 (Agencywide Documents Access and Management System (ADAMS) Accession No. ML16252A207), the U.S. Nuclear Regulatory Commission (NRC) issued Amendment No. 234 to Facility Operating License No. NPF-10 and Amendment No. 227 to Facility Operating License No. NPF-15 for the San Onofre Nuclear Generating Station (SONGS), Units 2 and 3, respectively. The amendments were issued in response to a letter from Southern California Edison (SCE, the licensee) dated June 16, 2016 (ADAMS Accession No. ML16172A075), as supplemented by letter dated September 6, 2016 (ADAMS Accession No. ML16252A288).

Amendment Nos. 234 and 227 allow for a revised schedule for implementation of the SONGS Cyber Security Plan (CSP) Milestone 8 and revised Paragraph 2.E in each of the Facility Operating Licenses to reflect this amended schedule. The SONGS CSP and associated implementation schedule for SONGS, Units 2 and 3, were previously approved by the NRC staff by letter dated July 28, 2011 (ADAMS Accession No. ML111960323), and further modified by letter dated October 1, 2015 (ADAMS Accession No. ML15209A935).

Subsequent to the issuance of the January 23, 2017, license amendment, SCE submitted an email dated January 25, 2017 (ADAMS Accession No. ML17038A190), notifying the NRC that during its review and implementation of the associated safety evaluation (SE) SCE identified a potential issue in need of clarification between the SCE submittal and the NRC's subsequent SE. A description, discussion, and disposition for this item are provided below.

Clarification – Scope of Cyber Remediation Activities

Section 3.2 of the NRC safety evaluation dated January 23, 2017, states:

> The NRC staff further finds that the licensee's request to delay final implementation of the CSP until December 31, 2019, is reasonable. In reaching this finding, the staff considered: (1) the need to perform design changes during

> decommissioning activities; (2) the status of the plant and the cyber security program; **(3) the completion of the cyber security remediation of the Plant Security System** [emphasis added]; (4) the reduced fire risk; (5) the time since last reactor operation; and (6) the significantly reduced risk profile presented by SONGS in the permanently shutdown and defueled configuration. Therefore, the NRC has reasonable assurance that full implementation of the CSP by December 31, 2019, will provide adequate protection of the public health and safety and the common defense and security.

Section 3.4 of the SE further states:

> The NRC staff has determined that the licensee's request to delay full implementation of its CSP until December 31, 2019, is reasonable for the following reasons: (i) the licensee's implementation of Milestones 1 through 7 already provides mitigation for significant cyber attack vectors for the most significant CDAs, as discussed above; (ii) the status of the cyber security program, **the completion of the cyber security remediation of the Plant Security System** [emphasis added], the significantly reduced risk profile presented by SONGS in the permanently shutdown configuration, and the time since last reactor operation ensures that SONGS is cyber secure; (iii) the licensee has reasonably prioritized and scheduled the work required to come into full compliance with its CSP implementation schedule; (iv) the scope of the work required to come into full compliance with the CSP implementation schedule was much more complicated than anticipated and not reasonably foreseeable when the CSP implementation schedule was originally developed; and (v) the licensee is utilizing tools to sufficiently manage the impact of the requested additional implementation time on the overall CSP.

However, the licensee's January 25, 2017, correspondence notes that paragraph item (3) in Section 3.2 and a portion of paragraph item (ii) in Section 3.4 would be more accurate if they referenced cyber security remediation efforts associated with the Spent Fuel Pool Cooling System and not the Plant Security System. This is more consistent with the description of the scope of the cyber security assessment and remediation activities included in SCE's application, as supplemented, and better describes the current configuration of the decommissioning facility.

The NRC staff has evaluated the significance of replacing the reference to the Plant Security System in these two paragraphs with the Spent Fuel Pool Cooling System on the conclusions reached in the SE regarding the adequacy of cyber security remediation activities, and determined that there is no safety impact associated with this change. The staff notes that during the review of the subject amendment request it was understood that the only systems that remained active now that the plant has entered decommissioning are the Spent Fuel Pool, Spent Fuel Pool Cooling System, and portions of the Plant Security System which protect the pool and its cooling system. As stated in the licensee's application, the computer and communication systems and networks including the Plant Security System remain adequately protected against cyber-attacks. Therefore, the conclusion in the NRC SE that full implementation of the SONGS CSP by December 31, 2019, will provide adequate protection of the public health and safety and the common defense and security, remains valid.

Given the above considerations, the NRC is issuing two revised SE pages to remove the statements describing the Plant Security System and replace them with the Spent Fuel Pool Cooling System in order to prevent future confusion. Enclosed please find a corrected Page 7 and a corrected Page 8 of the NRC's SE, which implements these changes as described.

If there are additional questions regarding any of the above corrections or clarifications, please contact me at 301-415-3178, or via email at marlayna.vaaler@nrc.gov.

Sincerely,

/RA/

Marlayna Vaaler, Project Manager
Reactor Decommissioning Branch
Division of Decommissioning, Uranium Recovery,
and Waste Programs
Office of Nuclear Material Safety and Safeguards

Docket Nos. 50-361 and 50-362

Enclosure:
As stated

cc w/encl: Distribution via Listserv

San Onofre Nuclear Generating Station, Units 2 and 3 – Correction Letter for License Amendment Nos. 234 and 227 Regarding Revision of the Cyber Security Plan Milestone 8 Completion Date in the Facility Operating Licenses (CAC Nos. L53132 and L53133) **– February 24, 2017**

DISTRIBUTION:
PUBLIC RDB r/f RBrowder, RIV

ADAMS Accession No. ML17053B490 ***via email**

OFFICE	NMSS/RDB/PM	NMSS/DUWP/LA	NSIR/CSD	NMSS/RDB/BC
NAME	MVaaler	CHolston	JRycyna*	BWatson
DATE	2/14/2017	2/22/2017	2/16/2017	2/24/17

OFFICIAL RECORD COPY

8) A discussion of modifications completed to support the cyber security program and a discussion of pending cyber security modifications.

The licensee provided a brief discussion of completed modifications and pending modifications, including those related to ISFSI security in support of the CSP, which will be based on completion of the CDA assessments currently in progress.

3.2 NRC Staff Evaluation of Requested Change

The NRC staff evaluated the licensee's application, as supplemented, using the regulatory requirements and guidance cited in Section 2.0 of this Safety Evaluation. The licensee stated that the CSP requirement regarding additional time to implement is found in CSP, Section 3.1, "Analyzing Digital Computer Systems and Networks Applying Cyber Security Controls." The licensee provided a list of additional activities required to implement the CSP requirement.

The licensee indicated in its application that completed activities associated with the CSP, as described in Milestones 1 through 7, and completed prior to December 31, 2012, provide a high degree of protection and that the most significant digital computer and communication systems and networks associated with SSEP systems are already protected against cyber attacks while SONGS implements the full program. The licensee also detailed activities completed for each milestone and provided details about the completed milestones and elements. On this basis, the NRC staff finds that the licensee's site is more secure after implementation of Milestones 1 through 7 at SONGS because the activities that the licensee completed will mitigate the most significant cyber attack vectors for the most significant CDAs. In addition, the site is more secure because of the significantly reduced risk profile presented by SONGS in the permanently shutdown and defueled configuration.

The licensee proposed a Milestone 8 completion date of December 31, 2019. The NRC staff has had extensive interaction with the nuclear industry since licensees first developed their CSP implementation schedules. Based on this interaction, the NRC staff recognizes that CDA assessment work is much more complex and resource-intensive than originally anticipated. In addition, due to the unplanned permanent shutdown of SONGS, Units 2 and 3, the licensee has a large number of additional tasks that it did not consider when it originally developed its CSP implementation schedule. The NRC staff concludes that the licensee's request for additional time to implement Milestone 8 is reasonable, given the effectiveness of the SONGS CSP with Milestones 1 through 7 already in place, the reduced risk profile in the permanently shutdown configuration, and the unanticipated complexity and scope of work required to come into full compliance with the current CSP.

The NRC staff further finds that the licensee's request to delay final implementation of the CSP until December 31, 2019, is reasonable. In reaching this finding, the staff considered: (1) the need to perform design changes during decommissioning activities; (2) the status of the plant and the cyber security program; (3) the completion of the cyber security remediation of the Spent Fuel Pool Cooling System; (4) the reduced fire risk; (5) the time since last reactor operation; and (6) the significantly reduced risk profile presented by SONGS in the permanently shutdown and defueled configuration. Therefore, the NRC has reasonable assurance that full implementation of the CSP by December 31, 2019, will provide adequate protection of the public health and safety and the common defense and security.

3.3 Revision to License Conditions

By letter dated June 16, 2016, the licensee proposed to modify Paragraph 2.E of Facility Operating License Nos. NPF-10 and NPF-15 with a license condition requiring the licensee to fully implement and maintain in effect all provisions of the NRC-approved CSP.

The licensee proposed to modify part of License Condition 2.E of Facility Operating License No. NPF-10, as follows:

> SCE shall fully implement and maintain in effect all provisions of the Commission-approved cyber security plan (CSP), including changes made pursuant to the authority of 10 CFR 50.90 and 10 CFR 50.54(p). The SONGS CSP was approved by License Amendment No. 225, as supplemented by changes approved by License Amendments 231 and 234.

The licensee proposed to modify part of License Condition 2.E of Facility Operating License No. NPF-15, as follows:

> SCE shall fully implement and maintain in effect all provisions of the Commission-approved cyber security plan (CSP), including changes made pursuant to the authority of 10 CFR 50.90 and 10 CFR 50.54(p). The SONGS CSP was approved by License Amendment No. 218, as supplemented by changes approved by License Amendments 224 and 227.

3.4 Summary of Technical Evaluation

The NRC staff has determined that the licensee's request to delay full implementation of its CSP until December 31, 2019, is reasonable for the following reasons: (i) the licensee's implementation of Milestones 1 through 7 already provides mitigation for significant cyber attack vectors for the most significant CDAs, as discussed above; (ii) the status of the cyber security program, the completion of the cyber security remediation of the Spent Fuel Pool Cooling System, the significantly reduced risk profile presented by SONGS in the permanently shutdown configuration, and the time since last reactor operation ensures that SONGS is cyber secure; (iii) the licensee has reasonably prioritized and scheduled the work required to come into full compliance with its CSP implementation schedule; (iv) the scope of the work required to come into full compliance with the CSP implementation schedule was much more complicated than anticipated and not reasonably foreseeable when the CSP implementation schedule was originally developed; and (v) the licensee is utilizing tools to sufficiently manage the impact of the requested additional implementation time on the overall CSP.

Based on its review of the application, as supplemented, the NRC staff concludes that the licensee's implementation of Milestones 1 through 7 has added additional protection that provides mitigation for significant cyber attack vectors for the most significant CDAs, that the licensee's explanation of the need for additional time to complete Milestone 8 given the transfer to an ISFSI-only configuration by the end of 2019, is compelling, and that it is acceptable for the licensee to complete implementation of Milestone 8, full implementation of the CSP, by December 31, 2019. The NRC staff also concludes that, upon full implementation of the licensee's cyber security program, the requirements of the licensee's CSP and 10 CFR 73.54