10 CFR 50.90

MARIA L. LACAL
Senior Vice President, Nuclear
Regulatory & Oversight

Palo Verde
Nuclear Generating Station
P.O. Box 52034
Phoenix, AZ 85072
Mail Station 7605
Tel 623.393.6491

102-07411-MLL/TNW
June 14, 2017

U. S. Nuclear Regulatory Commission
ATTN: Document Control Desk
Washington, DC 20555-0001

Dear Sirs:

Subject: **Palo Verde Nuclear Generating Station**
Units 1, 2 and 3
Docket Nos. STN 50-528, 50-529, and 50-530
Renewed Operating License Nos. NPF-41, NPF-51 and NPF-74
License Amendment Request for Revision to the Cyber Security Plan Implementation Schedule Completion Date

By letter dated July 26, 2011 [Agency Documents Access and Management System (ADAMS) Accession Number ML111710110], the NRC staff issued license amendment number 185 that approved the Palo Verde Nuclear Generating Station (PVNGS) Cyber Security Plan. The license amendment contained the following provision:

> "All subsequent changes to the NRC-approved CSP implementation schedule will require prior NRC approval pursuant to 10 CFR 50.90"

Consistent with this provision, Arizona Public Service Company (APS) submitted a license amendment request (LAR) to modify the Cyber Security Plan implementation of Milestones 6 and 7, and received NRC approval by license amendment number 190, dated December 13, 2013 (ADAMS Accession Number ML12312A186). APS has recently identified the need to modify the completion date for implementation of Milestone 8 of the PVNGS Cyber Security Plan. Therefore, in accordance with the provisions of Section 50.90 of Title 10 of the *Code of Federal Regulations* (10 CFR), APS is submitting this LAR for an extension of the Milestone 8 completion date from September 30, 2017, to December 31, 2017.

The enclosure to this letter provides a description and assessment of the proposed change including a summary of the technical evaluation, a regulatory evaluation, a no significant hazards consideration determination, and an environmental consideration.

In accordance with the PVNGS Quality Assurance Program Description, the Plant Review Board and the Offsite Safety Review Committee have reviewed and approved this LAR. By copy of this letter, this LAR is being forwarded to the Arizona Radiation Regulatory Agency in accordance with 10 CFR 50.91(b)(1).

APS plans to revise an existing commitment to fully implement the PVNGS Cyber Security Plan by December 31, 2017, as described in the enclosure to this letter.

APS requests approval of the LAR prior to the expiration of the current Milestone 8 completion date of September 30, 2017. APS will implement the amendment prior to September 30, 2017.

Should you have any questions concerning the content of this letter, please contact Michael DiLorenzo, Section Leader, Nuclear Regulatory Affairs, at (623) 393-3495.

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

Executed on: June 14, 2017
(Date)

Sincerely,

Lacal, Maria L(Z06149) Digitally signed by Lacal, Maria L(Z06149)
DN: cn=Lacal, Maria L(Z06149)
Date: 2017.06.14 11:04:30 -07'00'

MLL/TNW/CJS/sma

Enclosure: Description and Assessment of Proposed License Amendment

cc:

	K. M. Kennedy	NRC Region IV Regional Administrator
	S. P. Lingam	NRC NRR Project Manager for PVNGS
	M. M. Watford	NRC NRR Project Manager
	C. A. Peabody	NRC Senior Resident Inspector for PVNGS
	T. Morales	Arizona Radiation Regulatory Agency (ARRA)

Enclosure

Description and Assessment of Proposed License Amendment

CONTENTS

1.0 SUMMARY DESCRIPTION

By letter dated July 26, 2011 [Agency Documents Access and Management System (ADAMS) Accession Number ML111710110], the Nuclear Regulatory Commission (NRC) staff issued license amendment number 185 that approved the Palo Verde Nuclear Generating Station (PVNGS) Cyber Security Plan (Reference 1). The license amendment contained the following provision:

> "All subsequent changes to the NRC-approved CSP implementation schedule will require prior NRC approval pursuant to 10 CFR 50.90"

Consistent with this provision, Arizona Public Service Company (APS) submitted a license amendment request (LAR) to modify the Cyber Security Plan implementation of Milestones 6 and 7, and received NRC approval by license amendment number 190, dated December 13, 2013 (ADAMS Accession Number ML12312A186). APS has recently identified the need to modify the completion date for implementation of Milestone 8 of the PVNGS Cyber Security Plan. Therefore, in accordance with the provisions of Section 50.90 of Title 10 of the *Code of Federal Regulations* (10 CFR), APS is submitting this LAR for an extension of the Milestone 8 completion date from September 30, 2017, to December 31, 2017.

This enclosure provides a description and assessment of the proposed change including a summary of the technical evaluation, a regulatory evaluation, a no significant hazards consideration determination, and an environmental consideration.

2.0 DETAILED DESCRIPTION

2.1 Proposed Change to the PVNGS Operating Licenses

APS is submitting this LAR to extend the Milestone 8 completion date from September 30, 2017, to December 31, 2017. Specifically, this LAR requests that the current Cyber Security license condition (PVNGS Units 1, 2 and 3, renewed Operating License paragraph 2.E) be modified to reflect this license amendment requested to approve the Milestone 8 extension, as follows:

> APS 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 APS CSP was approved by License Amendment No. 185 as supplemented by a change approved by License Amendment No. 190 and a change approved by License Amendment No. XXX.

2.2 Need for Proposed Change

The proposed LAR is needed since APS has identified that additional time is required to complete the implementation of Milestone 8 of the PVNGS Cyber Security Plan. The following Section 3.0, *Technical Evaluation*, provides further details on the need for the proposed change

3.0 TECHNICAL EVALUATION

In Reference 3, the NRC staff provided eight criteria to be used for evaluation of a license amendment request to revise the Cyber Security Plan Implementation Schedule Milestone 8

date. These criteria serve to explain the current status of the PVNGS cyber security program and the need for the Implementation Milestone 8 completion date revision.

Below is the APS discussion of the eight evaluation criteria provided by Reference 3:

1) **Identification of the specific requirements of the cyber security plan that APS needs additional time to implement.**

   The PVNGS Cyber Security Plan, Appendix A, Sections 3 and 4, describe requirements for application and maintenance of cyber security controls listed in Appendices D and E of Nuclear Energy Institute (NEI) 08-09 Revision 6, *Cyber Security Plan for Nuclear Power Reactors* (Reference 5). Application of the controls is accomplished after completion of detailed analyses (the cyber security assessment process) that identify 'gaps' or the difference between current configuration and a configuration that satisfies each cyber security control. Gap closure can require any combination of physical, logical (software-related), or programmatic/procedural changes. Specific requirements needing additional time include:

   a. APS currently has a fast track modification in progress for the Meteorological Data Transmission System (MDTS) to apply cyber security controls pursuant to NEI 08-09, Revision 6, Appendix D.

   b. Ongoing assessment and application of cyber security controls for the recently modified Security System (SK-305).

   c. Programmatic change management associated with approximately 30 procedure changes pursuant to NEI 08-09, Revision 6, Appendix E.

2) **Detailed justification that describes the reason APS requires additional time to implement the specific requirements identified.**

   a. During the fourth quarter of 2016, cyber security assessments concluded that the MDTS required a full system modification for compliance with NEI 08-09, Revision 6, Appendix D. The PVNGS Work Authorization (WA) process for the modification was approved and a fast-track modification created for the MDTS. The initial modification target completion date of September 30, 2017 was consistent with the existing Milestone 8. To date, contracts for system components and modification development have been issued, a modification kick-off meeting completed and work is in progress. While continuing to work towards the initial completion date, it has been determined that additional time to complete implementation of the modification will be required.

   b. In January 2017, APS completed installation of the Security System Upgrade Project (SK-305). The SK-305 project had been ongoing for several years and faced multiple challenges. Although the physical installation is complete, the project is still working towards creation of final configuration documentation. Due to the lack of final configuration documentation on the new security system it has delayed the cyber security assessment of the new security system. The new security system assessment is in progress and additional resources, including members from the SK-305 project, have been added to the security assessment team to finish the assessment and application of cyber security controls. Even with these supplemental resources, additional time is needed to complete the

assessments and implement any cyber security controls identified during the assessment.

c. The following items also contribute to the need for additional time to fully implement Milestone 8:

- Critical Digital Asset (CDA) mitigation activities defined in Appendix A, Section 3.1.6, of the Cyber Security Plan have proved to be resource intensive
- Remediation activities (i.e., controls) need to be carefully considered
- Incorporation of NRC endorsed Addendum 1 to NEI 08-09, Revision 6
- Change management challenges
- Training on new programs, processes, and procedures

3) A proposed completion date for Milestone 8 consistent with the remaining scope of work to be conducted and the resources available.

APS is requesting a change to the implementation completion date of Milestone 8 from September 30, 2017, to December 31, 2017, to complete CDA assessments, implement design modifications based on assessment results, update existing procedures, develop new program procedures and provide training to complete full implementation of the cyber security program.

4) An evaluation of the impact that the additional time to implement the requirements will have on the effectiveness of the PVNGS overall cyber security program in the context of milestones already completed.

The impact of the requested additional implementation time on the effectiveness of the overall cyber security program is considered to be very low because APS has completed the interim implementation Milestones 1 through 7, that were required to be completed by December 31, 2012, and Reference 6. The completed activities provide a high degree of protection against cyber attacks while APS implements the full program. The completed activities include:

a. A PVNGS Cyber Security Assessment Team (CSAT) has been implemented consisting of highly experienced personnel knowledgeable in reactor and balance-of-plant design, licensing, safety, security, emergency preparedness, information technology, and cyber security. The CSAT is provided with the authority, via written procedures, to perform the analyses and oversight activities described in the Cyber Security Plan.

b. Critical systems and CDAs have been identified, documented, and entered into the PVNGS records system.

c. The plant process computer network and the plant security computer network have been deterministically isolated per the requirements of the cyber security Interim Milestone 3.

d. Safety-related, important-to-safety, and security CDAs have been extensively reviewed and verified (or modified) to be deterministically isolated and not employ wireless technology.

e. Procedures have been implemented for portable digital media and devices periodically connected to CDAs, per NEI 08-09, Revision 6 (Reference 5), Appendix D, Section 1.19.

f. Employees have been provided training on cyber security awareness, tampering, and control of portable digital media and devices periodically connected to CDAs.

g. CDAs associated with physical security target sets have been analyzed per the requirements of the CSP Appendix A, Section 3.1.6, and verified to satisfy the technical cyber security controls described in NEI 08-09, Revision 6 (Reference 5), Appendix D.

h. An ongoing monitoring and assessment program has been implemented.

i. PVNGS has transitioned from the previous cyber security program described in NEI 04-04 to NEI 08-09, Revision 6 (Reference 5). Revisions have been made to procedures that control plant modifications, planning, and maintenance, establishing ties to the cyber security procedures for CDA analysis and control of portable digital media and devices periodically connected to CDAs.

5) A description of the APS methodology for prioritizing completion of work for critical digital assets associated with significant safety, security, or emergency preparedness consequences and with reactivity effects in the balance of plant.

The APS methodology for prioritizing the implementation of Milestone 8 activities is centered on considerations for safety, security, and emergency preparedness (SSEP) and Balance of Plant (BOP) continuity of power consequences. The methodology is based on defense-in-depth, installed configuration of the CDAs and susceptibility to the five commonly identified threat vectors listed in the NRC Cyber Security Significance Determination Process. Prioritization for CDA assessment begins with safety related CDAs and continues through the lower priority non-safety and emergency preparedness (EP) CDAs:

- Safety related CDAs
- Physical security CDAs
- Important to safety CDAs (including BOP CDAs that directly impact continuity of power) and control system CDAs
- Non-safety related CDAs and EP CDAs

The remainder of the implementation of Milestone 8 work listed below will be fully implemented by the revised December 31, 2017 completion date:

- Completion of the balance of the non-safety related and EP CDA assessments
- Completion of all individual security control design remediation actions including those that require a refueling outage for implementation and/or alternative controls put in place
- Completion of station procedure revisions (approximately 30) to integrate the cyber security program
- Completion of integration of on-going periodic and time based actions into the plant preventive maintenance/surveillance (or equivalent) programs

- Completion of implementation of the cyber security change management plan including any required training

6) A discussion of the PVNGS cyber security program performance up to the date of the license amendment request.

In October 2013, the NRC completed an inspection related to compliance with interim Milestones 1 through 7. All findings were found to meet the criteria described in Reference 6 for enforcement discretion, and were entered into the corrective action program. In June 2015, the NRC completed a Cyber Security Milestone 8 pilot assessment.

The PVNGS Nuclear Assurance Department (NAD) has performed audits for both interim Milestones 1 through 7 and for Milestone 8 compliance and has not found any significant items requiring immediate attention. Another Milestone 8 NAD audit will be conducted prior to the revised Milestone 8 completion date of December 31, 2017. Audit/assessment issues are entered into the corrective action program and addressed for program improvement.

On-going monitoring and time-based periodic actions provide continuing program performance monitoring.

7) A discussion of cyber security issues pending in the PVNGS corrective action program.

There are presently no significant (constituting a threat to a CDA via cyber means or calling into question program effectiveness) nuclear cyber security issues pending in the corrective action program. Several non-significant issues identified through self-identification, Security Frequently Asked Question (SFAQ) notification, industry lessons learned, and NAD audits have been entered into the corrective action program.

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

Modifications completed include installation of modifications associated with Milestone 3 in accordance with the Cyber Security Plan and associated defense-in-depth procedures. In addition, modifications that have completed for Milestone 8 include:

- PVNGS automated security information and event management (SIEM) system for monitoring activity on plant process computer network
- Cyber hardening of the Plant Computer system
- Cyber hardening of the generator excitation system

Pending modifications which will be completed prior to the revised December 31, 2017 date include:

- MDTS cyber security control system upgrade
- Cyber hardening of the modified plant security system

4.0 REGULATORY EVALUATION

4.1 Applicable Regulatory Requirements

10 CFR 73.54 requires licensees to maintain and implement a cyber security plan. The PVNGS Units 1, 2 and 3 Renewed Facility Operating Licenses include a physical protection license condition that requires APS to fully implement and maintain in effect all provisions of the Commission-approved cyber security plan, including changes made pursuant to the authority of 10 CFR 50.90 and 10 CFR 50.54(p).

4.2 Precedent

The proposed license amendment was developed using relevant information from an approved change (Reference 4) at another nuclear station.

Benchmarking data gathered on Milestone 8 implementation schedules for other licensees indicate that a significant number of licensees have obtained approval for a Milestone 8 completion date in December of 2017. Therefore, this request is consistent with the industry.

4.3 No Significant Hazards Consideration Determination

Pursuant to 10 CFR 50.90, *Application for amendment of license, construction permit, or early site permit*, Arizona Public Service Company (APS) hereby requests an amendment to the Renewed Facility Operating Licenses for Palo Verde Nuclear Generating Station (PVNGS) Units 1, 2 and 3. This amendment request proposes a change to the Implementation Milestone 8 completion date specified in the PVNGS Cyber Security Plan Implementation Schedule.

As required by 10 CFR 50.91(a), *Notice for Public Comment*, an analysis of the issue of no significant hazards consideration using the standards in 10 CFR 50.92, *Issuance of Amendment*, is presented below:

1. Does the proposed amendment involve a significant increase in the probability or consequences of an accident previously evaluated?

   Response: No.

   The proposed change to the PVNGS Cyber Security Plan implementation schedule is administrative in nature. This proposed change does not alter accident analysis assumptions, add any initiators, or affect the function of plant systems or the manner in which systems are operated, maintained, modified, tested, or inspected. The proposed change does not require any plant modifications which affect the performance capability of the structures, systems, and components (SSCs) relied upon to mitigate the consequences of postulated accidents, and has no impact on the probability or consequences of an accident previously evaluated.

   Therefore, the proposed change will not involve a significant increase in the probability or consequences of an accident previously evaluated.

2. Does the proposed amendment create the possibility of a new or different kind of accident from any accident previously evaluated?

Response: No.

The proposed change to the PVNGS Cyber Security Plan implementation schedule is administrative in nature. This proposed change does not alter accident analysis assumptions, add any initiators, or affect the function of plant systems or the manner in which systems are operated, maintained, modified, tested, or inspected. The proposed change does not require any plant modifications which affect the performance capability of the SSCs relied upon to mitigate the consequences of postulated accidents, and does not create the possibility of a new or different kind of accident from any accident previously evaluated.

Therefore, the proposed change does not create the possibility of a new or different kind of accident from any accident previously evaluated.

3. Does the proposed amendment involve a significant reduction in a margin of safety?

Response: No.

Plant safety margins are established through limiting conditions for operation, limiting safety systems settings, and safety limits specified in the technical specifications. The proposed change to the PVNGS Cyber Security Plan implementation schedule is administrative in nature. Since the proposed change is administrative in nature, there are no changes to these established safety margins.

Therefore, the proposed change does not involve a significant reduction in a margin of safety as defined in the basis for any TS.

4.4 Conclusions

APS concludes that operation of the facility in accordance with the proposed amendment does not involve a significant hazards consideration under the standards set forth in 10 CFR 50.92(c), and, accordingly, a finding of "no significant hazards consideration" is justified. Based on the considerations discussed above, (1) there is reasonable assurance that the health and safety of the public will not be endangered by operation in the proposed manner, (2) such activities will be conducted in compliance with the Commission's regulations, and (3) the issuance of the amendment will not be inimical to the common defense and security or the health and safety of the public.

5.0 ENVIRONMENTAL CONSIDERATION

A review has determined that the proposed amendment would change a requirement with respect to installation or use of a facility component located within the restricted area, as defined in 10 CFR 20, *Standards for Protection Against Radiation*. However, the proposed amendment does not involve (i) a significant hazards consideration, (ii) a significant change in the types or a significant increase in the amounts of any effluents that may be released offsite, or (iii) a significant increase in individual or cumulative occupational radiation exposure. Accordingly, the proposed amendment meets the eligibility criterion for categorical exclusion set forth in 10 CFR 51.22(c)(9). Therefore, pursuant to 10 CFR 51.22(b), no environmental impact statement or environmental assessment need be prepared in connection with the proposed amendment.

6.0 REFERENCES

1. NRC letter, *Palo Verde Nuclear Generating Station, Units 1, 2 and 3, Issuance of Amendments, RE: Approval of Cyber Security Plan*, dated July 26, 2011 (ADAMS Accession Number ML111710110)

2. NRC letter, *Palo Verde Nuclear Generating Station, Units 1, 2 and 3 – Issuance of amendments, RE: Change in Implementation of Cyber Security Plan,* dated December 13, 2013 (ADAMS Accession Number ML12312A186)

3. NRC Memorandum from R. Felts, USNRC to B. Westreich, USNRC, *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 Number ML13295A467)

4. NRC letter, *Wolf Creek Generating Station – Issuance of Amendment, RE: Revision to the Cyber Security Plan Implementation Schedule,* dated March 24, 2017 (ADAMS Accession Number ML17024A241)

5. Nuclear Energy Institute (NEI) 08-09, Revision 6, *Cyber Security Plan for Nuclear Power Reactors*" dated April 2010

6. NRC Memorandum from B. Westreich, USNRC, to T. Blount, USNRC, *Enhanced Guidance for Licensee Near-Term Corrective Actions to Address Cyber Security Inspection Findings and Licensee Eligibility for 'Good-Faith' Attempt Discretion*, dated July 1, 2013 (ADAMS Accession ML13178A203)