



A subsidiary of Pinnacle West Capital Corporation

Palo Verde Nuclear
Generating Station

Dwight C. Mims
Vice President
Regulatory Affairs and Plant Improvement

Tel. 623-393-5403
Fax 623-393-6077

Mail Station 7605
P. O. Box 52034
Phoenix, Arizona 85072-2034

102-06311-DCM/TLC
January 20, 2011

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

Dear Sirs:

**Subject: Palo Verde Nuclear Generating Station (PVNGS)
Units 1, 2, and 3
Docket Nos. STN 50-528, 50-529 and 50-530
Response to Request for Additional Information for the Review of the
PVNGS Cyber Security Plan**

By letter number 102-06226, dated July 22, 2010, Arizona Public Service Company submitted a request for approval of the PVNGS Cyber Security Plan (Agencywide Documents Access and Management System [ADAMS] Accession No. ML102150230). The U.S. Nuclear Regulatory Commission (NRC) staff, in a letter dated December 16, 2010, issued a request for additional information (RAI) related to the PVNGS Cyber Security Plan submittal.

The enclosure to this letter contains Arizona Public Service Company's (APS's) response to the RAIs. All three of the RAIs were related to deviations from the NEI-provided template that APS had taken in its July 22, 2010, submittal.

After reviewing the RAI questions, APS has decided to restore the wording of the PVNGS Cyber Security Plan in all three instances to conform with the NEI template. In one case, a sentence will be added to clarify APS's position on handling of cyber security vulnerabilities. These RAI responses will require changes in the license amendment request (LAR) for the PVNGS Cyber Security Plan. The PVNGS Cyber Security Plan submittal will be revised to include the plant specific changes identified in this RAI response at the same time as the change to describe jurisdiction of balance of plant systems, structures, and components (SSCs), as described in letter 102-06288, dated November 30, 2010.

No commitments are being made by this letter. Should you need further information regarding this response, please contact Russell A. Stroud, Licensing Section Leader, at (623) 393-5111.

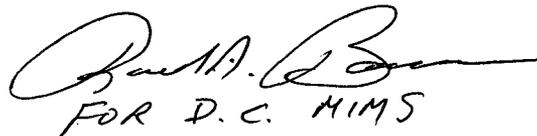
SDDIA
HRR

ATTN: Document Control Desk
U.S. Nuclear Regulatory Commission
Response to Request for Additional Information for the Review of the PVNGS Cyber
Security Plan
Page 2

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

Executed on JANUARY 20, 2011
(date)

Sincerely,



FOR D. C. HIMS

DCM/RAS/TLC/gat

Enclosure: APS Response to NRC Request for Additional Information Regarding
PVNGS Cyber Security Plan Submittal

cc: E. E. Collins Jr. NRC Region IV Regional Administrator
J. R. Hall NRC NRR Senior Project Manager
L. K. Gibson NRC NRR Project Manager
M. A. Brown NRC Senior Resident Inspector for PVNGS
A. V. Godwin Arizona Radiation Regulatory Agency
T. Morales Arizona Radiation Regulatory Agency

Sr. Physical Security Inspector, RIV/DRS/PSB

ENCLOSURE

**APS Response to NRC Request for Additional Information
Regarding PVNGS Cyber Security Plan Submittal**

APS RESPONSE TO NRC REQUEST FOR ADDITIONAL INFORMATION (RAI)
REGARDING PVNGS CYBER SECURITY PLAN SUBMITTAL

By letter dated July 22, 2010, as supplemented by letters dated September 29 and November 30, 2010, Arizona Public Service Company (APS) submitted a license amendment request for approval of the Palo Verde Nuclear Generating Station (PVNGS) Cyber Security Plan (CSP).

On December 16, 2010, the Nuclear Regulatory Commission (NRC) staff requested the following additional information in support of the request for approval:

NRC Request 1:

Cyber Security Threat Evaluation (CSP Section 3.1.2: Cyber Security Assessment Team)

The NRC regulation in Title 10 of the *Code of Federal Regulations* (10 CFR) 73.54(d)(2) requires the licensee to evaluate and manage cyber risks. The PVNGS CSP Section 3.1.2, "Cyber Security Assessment Team," (CSAT) states, in part, that one of the roles and responsibilities of the CSAT is "Evaluating assumptions and conclusions about known cyber security threats; potential vulnerabilities to, and consequences from an attack; the effectiveness of existing cyber security controls, defensive strategies, and attack mitigation methods; cyber security awareness and training of those working with, or responsible for CDAs [critical digital assets] and cyber security controls throughout their system life cycles; ..." The above language deviates from the template by inserting the word "known" which could limit the scope of the CSAT evaluations.

Please explain how PVNGS uses the process described above to stay current on unknown or emerging cyber security threats.

APS Response to RAI #1:

APS will maintain awareness of current and emerging cyber security threats that could impact the nuclear industry in general and Palo Verde in particular. This will be accomplished by reviewing appropriate web sites (e.g. US CERT, etc.), regularly reviewing industry cyber security-related alerts, and by responding to those applicable to Palo Verde. The word "known" was inserted as a deviation to ensure it was understood that PVNGS could not protect against cyber security threats that were unknown and undetectable to the industry. Based on this common understanding, the LAR will be revised by removing: 1) the word "known" from the sentence in question, and 2) this specific deviation from the Deviation Table. The sentence in the PVNGS Cyber Security Plan will then read, "Evaluating assumptions and conclusions about

cyber security threats; potential vulnerabilities to, and consequences from an attack; the effectiveness of existing cyber security controls, defensive strategies, and attack mitigation methods; cyber security awareness and training of those working with, or responsible for CDAs [critical digital assets] and cyber security controls throughout their system life cycles; ..." APS will incorporate this change in the LAR with the Cyber Security Plan supplement that will be submitted to the NRC to clarify jurisdiction of balance of plant systems, structures, and components (SSCs), as described in letter 102-06288, dated November 30, 2010.

NRC Request 2:

Mitigation and Incident Response for Non-Remote Attacks (CSP Section 4.6: Attack Mitigation and Incident Response)

The NRC regulation in 10 CFR 73.54(a) requires the licensee to "provide high assurance that digital computer and communication systems and networks are adequately protected against cyber attacks, up to and including the design basis threat as described in §73.1." The regulations in 10 CFR 73.54(e)(2) require the licensee's cyber security program to "include measures for incident response and recovery for cyber attacks." Section 4.6, "Attack Mitigation and Incident Response," of the PVNGS CSP states "Policies, procedures, and programs (as outlined in the PVNGS Cyber Security Program) document cyber security controls to deny, deter, and detect adverse threats and conditions to CDAs that may be susceptible to remote cyber attacks which exploit system vulnerabilities." PVNGS deviated from the template in NEI 08-09, Rev. 6, "Cyber Security Plan for Nuclear Reactors," by inserting the word "remote" which could exclude insider attacks from consideration.

Please explain how the PVNGS will deny, deter, and detect threats and conditions to CDAs that may be susceptible to cyber attacks which are not remote (e.g., on-site).

APS Response to RAI #2:

APS will revise the LAR by removing: 1) the word "remote" from the sentence in question, and 2) this specific deviation from the Deviation Table. The sentence in the PVNGS Cyber Security Plan will then read, "Policies, programs, and procedures (as outlined in the PVNGS Cyber Security Program) document cyber security controls to deny, deter, and detect adverse threats and conditions to CDAs that may be susceptible to cyber attacks which exploit system vulnerabilities." APS will incorporate this change in the LAR with the Cyber Security Plan supplement that will be submitted to the NRC to clarify jurisdiction of balance of plant SSCs, as described in letter 102-06288, dated November 30, 2010.

NRC Request 3:

Eliminate vs. Mitigate Flaws in CDAs (CSP Appendix E: Operational and Management Cyber Security Controls (Section 3.2 of Appendix E))

The NRC regulation in 10 CFR 73.54(a)(1) requires that "the licensee shall protect digital computer and communication systems and networks associated with: (i) Safety-related and important-to-safety functions; (ii) Security functions; (iii) Emergency preparedness functions, including offsite communications"; and 10 CFR 73.54(c)(1) requires that the cyber security program must be designed to "implement security controls to protect the assets identified by paragraph (b)(1) of this section from cyber attacks." Furthermore, 10 CFR 73.54(d)(3) requires the licensee to "ensure that modifications to assets, identified by paragraph (b)(1) of this section, are evaluated before implementation to ensure that the cyber security performance objectives identified in paragraph (a)(1) of this section are maintained."

The PVNGS CSP, Deviation Table, suggests that Section 3.2 of Appendix E be changed. The current text reads, "Perform vulnerability scans or assessments of the CDA to validate that the flaw has been eliminated before the CDA is put into production." The deviation suggested is to replace the word 'eliminated' with the word 'mitigated.' The rationale for this change was that "It is very unlikely that there will be a case where the 'flaws' themselves can be completely 'eliminated.'" The proposed action in the revised PVNGS CSP would be to mitigate any flaws prior to equipment installation.

Please describe the processes, methods, and considerations to mitigate (which means to become less harsh or less severe) rather than eliminate (which means to remove) flaws before a compromised CDA is put back into production. If alternative controls are used, please explain the process and provide the criteria for selecting alternate controls to mitigate rather than eliminate any flaws in a CDA and clarify that the justification process provides equivalent protection in lieu of the security controls from Appendices D and E that cannot be implemented.

APS Response to RAI #3:

In order to clarify Palo Verde's handling of vulnerabilities, the word "eliminated" will be restored in that sentence of the PVNGS Cyber Security Plan and a new sentence will be added that further explains the process. APS plans to eliminate the cyber security vulnerabilities identified at Palo Verde as part of its ongoing Cyber Security Program. Where a cyber security vulnerability cannot be eliminated at Palo Verde, appropriate actions will be taken to mitigate the vulnerability. In response to this RAI, APS will revise the LAR Deviation Table to read as follows: "Perform vulnerability scans or assessments of the CDA to validate that the flaw has been eliminated before the CDA is

Enclosure
APS Response to NRC RAI for
PVNGS Cyber Security Plan Submittal

put into production. Where a vulnerability cannot be eliminated (using the resources normally available to a commercial nuclear facility) alternate controls or mitigating actions will be utilized." APS will incorporate this change in the LAR with the Cyber Security Plan supplement that will be submitted to the NRC to clarify jurisdiction of balance of plant SSCs, as described in letter 102-06288, dated November 30, 2010.