UNITED STATES

NUCLEAR REGULATORY COMMISSION

REGION *IV*
1600 EAST LAMAR BOULEVARD
ARLINGTON, TEXAS 76011-4511

January 10, 2024

Adam C. Heflin, Executive Vice President
Chief Nuclear Officer
Arizona Public Service Company
P.O. Box 52034, MS 7602
Phoenix, AZ 85072-2034

SUBJECT: PALO VERDE NUCLEAR GENERATING STATION, UNITS 1, 2, AND 3 - INFORMATION REQUEST FOR THE CYBERSECURITY BASELINE INSPECTION, NOTIFICATION TO PERFORM INSPECTION (05000528/2024404; 05000529/2024404; 05000530/2024404)

Dear Adam Heflin:

On May 20, 2024, the U.S. Nuclear Regulatory Commission (NRC) will begin a baseline inspection in accordance with Inspection Procedure (IP) 71130.10 “Cybersecurity,” at your Palo Verde Nuclear Generating Station, Units 1, 2, and 3. The inspection will be performed to evaluate and verify your ability to meet the requirements of the NRC’s Cybersecurity Rule, Title 10, *Code of Federal Regulations* (CFR), Part 73, Section 54, “Protection of Digital Computer and Communication Systems and Networks.”

Experience has shown that baseline inspections are extremely resource intensive, both for the NRC inspectors and licensee staff. In order to minimize the inspection impact on the site and to ensure a productive inspection for both parties, we have enclosed a request for documents needed for the inspection. These documents have been divided into four groups.

The first group specifies information necessary to assist the inspection team in choosing the focus areas (i.e., “sample set”) to be inspected by the IP 71130.10. This information should be made available either in an online repository (preferred) or digital media (CD/DVD) and delivered/available to the regional office no later than March 22, 2024. The inspection team will review this information and, by April 19, 2024, will request the specific items that should be provided for review.

The second group of requested documents will assist the inspection team in the evaluation of the critical systems and critical digital assets (CSs/CDAs), defensive architecture, and the areas of your cyber security program selected for review. This information will be requested for review in the regional office prior to the inspection by May 3, 2024, as identified above.

The third group of requested documents consists of additional items that the inspection team will review, or need access to, during the inspection. Please have this information available by the first day of the onsite inspection, May 20, 2024.

The fourth group of information aids the inspection team in tracking issues identified during the inspection. It is requested that this information be provided to the lead inspector as the information is generated during the inspection. It is important that all requested documents are up to date and complete to minimize the number of additional documents requested during the preparation and/or the onsite portions of the inspection.

The lead inspector for this inspection is Sam Graves. We understand that our regulatory contact for this inspection is Jeremia Mueller of your organization. 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

Paperwork Reduction Act Statement

This letter contains mandatory information collections that are subject to the Paperwork Reduction Act of 1995 (44 U.S.C. 3501 et seq.). The Office of Management and Budget (OMB) approved these information collections under approval number 3150-0011. The burden to the public for these information collections is estimated to average 40 hour(s) per response. Send comments regarding this information collection to the FOIA, Library and Information Collection Branch, Office of the Chief Information Officer, Mail Stop: T6-A10M, U.S. Nuclear Regulatory Commission, Washington, DC 20555-0001, or by email to Infocollects.Resource@nrc.gov, and to the Desk Officer, Office of Information and Regulatory Affairs, NEOB-10202, (3150-0011) OMB, Washington, DC 20503.

Public Protection Notification

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, “Public Inspections, Exemptions, Requests for Withholding,” 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’s Public Document Room or from the Publicly Available Records (PARS) component of the NRC's Agencywide Documents Access and Management 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,

/S/ Graves Signed by Graves, Samuel on 01/10/24

Sam Graves, Senior Reactor Inspector
Engineering Branch 2
Division of Operating Reactor Safety

Docket Nos. 05000528, 05000529, 05000530
License Nos. NPF-41, NPF-51, NPF-74
Enclosure: Palo Verde Nuclear Generating Station, Units 1, 2, And 3
Cyber-Security Inspection Document Request

cc w/encl: Distribution via LISTSERV®

PALO VERDE NUCLEAR GENERATING STATION, UNITS 1, 2, AND 3 - INFORMATION REQUEST FOR THE “CYBER-SECURITY” BASELINE INSPECTION, NOTIFICATION TO PERFORM INSPECTION 05000528/2024404; 05000529/2024404; 05000530/2024404 – DATED JANUARY 10, 2024

DISTRIBUTION:
JMonninger, ORA
JLara, ORA
GMiller, DORS
MHay, DORS
DCylkowski, RC
JHamman, RIV/OEDO
VDricks, ORA
LWilkins, OCA
DGalvin, NRR
AMoreno, RIV/OCA
RAlexander, RSLO
JDixon, DORS
ASanchez, DORS
LMerker, DORS
NCuevas, DORS
ELantz, DORS
YDubay, DORS
R4-DORS-IPAT
R4Enforcement
SOSB Insp Rpt Distro
SOSBInspRptDistro@usnrc.onmicrosoft.com

NTaylor, DORS
GDentel, DORS, RI
GMcCoy, DRS, RII
RSkowowski, DRS, RIII
BYip, DPCP, NSIR
TRivera, DPCP, NSIR
KLawson-Jenkins, DPCP, NSIR
TKeene, DSO, NSIR
DJohnson, DSO, NSIR
JRey, DSO, NSIR

ADAMS ACCESSION NUMBER: ML24010A153

☒ SUNSI Review:	ADAMS:	☐ Non-Publicly Available	☒ Non-Sensitive	Keyword:
By:	☒ Yes ☐ No	☒ Publicly Available	☐ Sensitive	NRC-002

OFFICE	RIV:SRI/DORS/EB2			
NAME	S. Graves			
SIGNATURE	/**RA/**			
DATE	01/10/24			

OFFICIAL RECORD COPY

PALO VERDE NUCLEAR GENERATING STATION
CYBERSECURITY INSPECTION DOCUMENT REQUEST

Inspection Report: 05000528/2024404; 05000529/2024404; 05000530/2024404

Inspection Dates: Week of May 20, 2024

Inspection Procedure: IP 71130.10, "CYBERSECURITY"

Reference: ML21330A088, "Guidance Document for Development of the Request for Information (RFI) and Notification Letter for IP 71130.10 Cyber Security Inspection," Revision 2

NRC Inspectors:

Sam Graves, Lead
817-200-1102
samuel.graves@nrc.gov

Andrew Saunders
817-200-1275
Andrew.saunders@nrc.gov

NRC CSB Staff:

Mario Fernandez
301-287-3687
Mario.fernandez@nrc.gov

NRC Contractors:

Trace Coleman
301-415-7000
Trace.coleman@nrc.gov

TBD

I. Information Requested for In-Office Preparation

This initial request for information (i.e., Table RFI #1) concentrates on providing the inspection team with information necessary to select appropriate components and cyber security program elements to develop a site-specific inspection plan. The first RFI is used to identify the critical digital assets or systems to be chosen as the "sample set" required to be inspected by the cyber-security IP. The first RFI's requested information is specified below in Table RFI #1. Please provide the information requested in Table RFI #1 to the regional office by March 22, 2024, or sooner, to facilitate the selection of the specific items for review.

The inspection team will examine the documentation from the first RFI and select specific systems and equipment to provide a more focused follow-up request to develop the second RFI. The inspection team will submit the specific systems and equipment list to your staff by April 19, 2024, which will be utilized to evaluate the equipment, defensive architecture, and the areas of the licensee's cyber security program for review.

Please provide the information requested by the second RFI to the regional office by

May 3, 2024. All requests for information shall follow the guidance document referenced above. For information requests that have more than ten (10) documents, please provide a compressed (i.e., Zip) file of the documents.
The required Table RFI #1 information shall be provided in an online document repository (preferred) or on digital media (CD/DVD) to the lead inspector by March 22, 2024. The preferred file format for all lists is a searchable Excel spreadsheet file. The information should be indexed and hyper-linked to facilitate ease of use. If you have any questions regarding this information, please contact the inspection team leader as soon as possible.

Table RFI #1		
Section 3, **Paragraph Number/Title:**		**IP Ref. Items**
1	A list of all Identified Critical Systems and Critical Digital Assets, – highlight/note any additions, deletions, reclassifications due to new guidance from white papers, changes to NEI 10-04, 13-10, etc. since the last cyber security inspection.	Overall
2	A list of EP and Security onsite and offsite digital communication systems	Overall
3	Network Topology Diagrams to include information and data flow for critical systems in levels 2, 3 and 4 (If available)	Overall
4	Ongoing Monitoring and Assessment program documentation	03.01(a)
5	The most recent effectiveness analysis and self-assessments of the Cyber Security Program	03.01(b)
6	Portable Media and Mobile Device control documentation, including kiosk security control assessment/documentation	03.02(e)
7	Design change/modification program documentation and a list of all cyber-related design changes completed since the last two cyber security inspections, including either a summary describing the design change or the 50.59 documentation for the change.	03.03(a)
8	Supply Chain Management documentation including any security impact analysis for new acquisitions	03.03(a), (b) and (c)
9	Cyber Security Plan and any 50.54(p) analysis to support changes to the plan since the last inspection	03.04(a)
10	Cyber Security Metrics tracked (if applicable)	03.06 (b)
11	Provide copies of all cybersecurity program related procedures and policies with their descriptive name and associated number (if available)	Overall

12	Performance testing report (if applicable)	03.06 (a)
13	Corrective actions taken as a result of cyber security incidents/issues to include previous NRC violations and Licensee Identified Violations since two last cyber security inspections	03.05

In addition to the above information please provide the following:

(1) Electronic copy of the UFSAR and technical specifications.

(2) Name(s) and phone numbers for the regulatory and technical contacts.

(3) Current management and engineering organizational charts.

Based on this information, the inspection team will identify and select specific systems and equipment (e.g., CSs/CDAs) from the information requested by Table RFI #1 and submit a list of specific systems and equipment to your staff by April 19, 2024, for the second RFI (i.e., RFI #2).

II. Additional Information Requested to be Available Prior to Inspection.

As stated in Section I above, the inspection team will examine the returned documentation requested from Table RFI #1 and submit the list of specific systems and equipment to your staff by April 19, 2024, for the second RFI (i.e., RFI #2). The second RFI will request additional information required to evaluate the CSs/CDAs, defensive architecture, and the areas of the licensee's CSP selected for the cybersecurity inspection. The additional information requested for the specific systems and equipment is identified in Table RFI #2. All requested information shall follow the guidance document referenced above.

The Table RFI #2 information shall be provided in an online document repository (preferred) or on digital media (CD/DVD) to the lead inspector by May 3, 2024. The preferred file format for all lists is a searchable Excel spreadsheet file. The information should be indexed and hyper-linked to facilitate ease of use. If you have any questions regarding this information, please contact the inspection team leader as soon as possible.

Table RFI #2		
Section 3, Paragraph Number/Title:		**IP Ref. Items**
	For the system(s) chosen for inspection provide:	
1	Ongoing Monitoring and Assessment activity performed on the system(s)	03.01(a)
2	All Security Control Assessments for the selected system(s)	03.01(a)

Table RFI #2		
Section 3, Paragraph Number/Title:		**IP Ref. Items**
3	All vulnerability screenings/assessments associated with, or scans performed on the selected system(s) since the last cyber security inspection	03.01(c)
4	Documentation (including configuration files and rules sets) for Network-based Intrusion Detection/Protection Systems (NIDS/NIPS), Host-based Intrusion Detection Systems (HIDS), and Security Information and Event Management (SIEM) systems for system(s) chosen for inspection	03.02(b)
5	Documentation (including configuration files and rule sets) for intra-security level firewalls and boundary devices used to protect or isolate the selected system(s)	03.02(c)
6	Copies of all periodic reviews of the access authorization list for the selected systems since the last inspection	03.02(d)
7	Baseline configuration information for the selected CDAs	03.03(a)
8	Documentation on any changes, including Security Impact Analyses, performed on the selected system(s) since the last inspection	03.03(b)
9	Copies of the purchase order documentation for any new equipment purchased for the selected systems since the last inspection	03.03(c)
10	Copies of any reports/assessment for cyber security drills performed since the last inspection.	03.02(a) 03.04(b)
11	Copy of the individual recovery plan(s) for the selected system(s) including documentation of the results the last time the backups were executed.	03.02(a) 03.04(b)
12	Vulnerability screening/assessment and scan program documentation	03.01(c)
13	Cyber Security Incident response documentation, including incident detection, response, and recovery documentation as well as contingency plan development, implementation and including any program documentation that requires testing of security boundary device functionality	03.02(a) and 03.04(b)
14	Device Access and Key Control documentation	03.02(c)
15	User Account/Credential documentation	03.02(d)
16	Password/Authenticator documentation	03.02(c)
17	Portable Media and Mobile Device control documentation, including kiosk security control assessment/documentation	03.02(e)

18	Configuration Management documentation including any security impact analysis performed due to configuration changes since the last inspection	03.03(a) and (b)
19	Provide documentation describing any cyber security changes to the access authorization program since the last cyber security inspection.	Overall

III. Information Requested to be Available on First Day of Inspection

For the specific systems and equipment identified in Section II above, provide the following RFI (i.e., Table - Onsite Week) to the team by May 20, 2024, the first day of the inspection. All requested information shall follow the guidance document referenced above.

The preferred file format for all lists is a searchable Excel spreadsheet file. The information should be indexed and hyper-linked to facilitate ease of use. If you have any questions regarding this information, please contact the inspection team leader as soon as possible.

Table - Onsite Week		
Section 3, Paragraph Number/Title:		**Items**
1	Any cyber security event reports submitted in accordance with 10 CFR 73.77 since the last cyber security inspection	03.04(a)
2	Updated Copies of corrective actions taken as a result of cyber security incidents/issues, to include previous NRC violations and Licensee Identified Violations since the last cyber security inspection, as well as vulnerability-related corrective actions	03.04(d)

In addition to the above information please provide the following:

(1) Copies of the following documents do not need to be solely available to the inspection team as long as the inspectors have easy and unrestrained access to them:

a. Updated Final Safety Analysis Report, if not previously provided;

b. Original SER and Supplements related to cybersecurity;

c. FSAR Question and Answers related to cybersecurity;

d. Quality Assurance Plan;

e. Technical Specifications, if not previously provided;

(2) Vendor Manuals, Assessments and Corrective Actions:

a. The most recent Cyber-Security Quality Assurance (QA) audit and/or self-assessment; and

b. Corrective action documents (e.g., condition reports, including status of corrective actions) generated as a result of the most recent Cyber-Security Quality Assurance (QA) audit and/or self-assessment.

IV. Information Requested To Be Provided Throughout the Inspection

(1) Copies of any corrective action documents generated as a result of the inspection team's questions or queries during the inspection.

(2) Copies of the list of questions submitted by the inspection team members and the status/resolution of the information requested (provided daily during the inspection to each inspection team member).

If you have any questions regarding the information requested, please contact the inspection team leader.