UNITED STATES
NUCLEAR REGULATORY COMMISSION
REGION I
2100 RENAISSANCE BOULEVARD, SUITE 100
KING OF PRUSSIA, PENNSYLVANIA 19406-2713

May 26, 2022

Mr. Brad Berryman
Senior Vice President and Chief Nuclear Officer
Susquehanna Nuclear, LLC
769 Salem Blvd., NUCSB3
Berwick, PA 18603

SUBJECT: SUSQUEHANNA STEAM ELECTRIC STATION, UNITS 1 AND 2 – INFORMATION REQUEST FOR THE CYBER SECURITY BASELINE INSPECTION, NOTIFICATION TO PERFORM INSPECTION 05000387/2022404 AND 05000388/2022404

Dear Mr. Berryman:

On October 3, 2022, the U.S. Nuclear Regulatory Commission (NRC) will begin a baseline inspection in accordance with Inspection Procedure (IP) 71130.10, "Cyber Security," dated December 14, 2021, at Susquehanna Steam Electric Station, Units 1 and 2. The inspection will be performed to evaluate and verify your ability to meet the requirements of the NRC's Cyber Security Rule, Title 10 of the *Code of Federal Regulations* (10 CFR) Part 73, Section 54, "Protection of Digital Computer and Communication Systems and Networks." The onsite portion of the inspection will take place October 3–7, 2022.

Experience has shown that baseline inspections are extremely resource intensive, both for the NRC inspectors and the 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 IP 71130.10. This information should be made available either on an online repository (preferred) or digital media (CD/DVD) no later than June 24, 2022. The inspection team will review this information and, by July 29, 2022, will request the specific items that should be provided for review.

The second group of additional 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 the licensee's Cyber Security Program selected for the cyber security inspection. This information will be requested for review in the regional office prior to the inspection by August 26, 2022, as identified above.

The third group of requested documents consists of those 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, October 3, 2022.

The fourth group of information is necessary to aid the inspection team in tracking issues identified as a result of 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 of these documents are up to date and complete in order 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 Louis Dumont. We understand that our regulatory contact for this inspection is Katie Brown of your organization. If there are any questions about the inspection or the material requested, please contact the lead inspector at 610-337-5183 or via e-mail at louis.dumont@nrc.gov.

This letter does not contain new or amended information collection requirements subject to the *Paperwork Reduction Act of 1995* (44 U.S.C. 3501 et seq.). Existing information collection requirements were approved by the Office of Management and Budget, control number 3150-0011. 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,

Glenn T. Dentel

Digitally signed by Glenn T. Dentel
Date: 2022.05.26 13:54:25 -04'00'

Glenn T. Dentel, Chief
Engineering Branch 2
Division of Operating Reactor Safety

Docket Nos. 05000387 and 05000388
License Nos. NPF-14 and NPF-22

Enclosure:
Cyber Security Inspection Document Request

cc: Distribution via ListServ

SUBJECT: SUSQUEHANNA STEAM ELECTRIC STATION, UNITS 1 AND 2 – INFORMATION REQUEST FOR THE CYBER SECURITY BASELINE INSPECTION, NOTIFICATION TO PERFORM INSPECTION 05000387/2022404 AND 05000388/2022404 DATED MAY 26, 2022

DISTRIBUTION:
JGreives, DORS
LCasey, DORS
EGarcia, DORS
CHighley, DORS, SRI
MRossi, DORS, RI
DHochmuth, DORS, AA
ROrlikowski, RI OEDO
RidsNrrPMSusquehanna Resource
RidsNrrDorlLpl1 Resource

DOCUMENT NAME: https://usnrc.sharepoint.com/teams/EngineeringBranch2/Shared Documents/Cyber Security/_Baseline Inspections/2022/Susquehanna/SQ Cyber Security RFI 1.docx
ADAMS ACCESSION NUMBER: ML22146A102

☑ SUNSI Review		☑ Non-Sensitive ☐ Sensitive		☑ Publicly Available ☐ Non-Publicly Available	
OFFICE	RI/DORS	RI/DORS			
NAME	LDumont	GDentel			
DATE	5/26/22	5/25/22			

OFFICIAL RECORD COPY

SUSQUEHANNA STEAM ELECTRIC STATION, UNITS 1 AND 2 CYBER SECURITY INSPECTION DOCUMENT REQUEST

Inspection Report: 05000387/2022404 AND 05000388/2022404

Inspection Dates: October 3–7, 2022

Inspection Procedure: IP 71130.10, "Cyber Security," dated December 14, 2021 (ADAMS Accession Number: ML21271A106)

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

NRC Inspectors:

Louis Dumont, Lead
610-337-5183
Louis.Dumont@nrc.gov

Manan Patel
610-337-5304
Manan.Patel@nrc.gov

Tim Hennessey
610-337-5135
Timothy.Hennessey@nrc.gov

NRC Contractors:

Casey Priester
Casey.Priester@nrc.gov

I. Information Requested for In-Office Preparation

The initial request for information (i.e., first RFI) concentrates on providing the inspection team with the general information necessary to select appropriate components and Cyber Security Program (CSP) elements to develop a site-specific inspection plan. The first RFI is used to identify the list of critical systems and critical digital assets (CSs/CDAs) plus operational and management (O&M) security control portions of the CSP to be chosen as the "sample set" required to be inspected by the cyber security inspection procedure. The first RFI's requested information is specified below in Table RFI #1. The Table RFI #1 information is requested to be provided to the regional office by June 24, 2022, or sooner, to facilitate the selection of the specific items that will be reviewed during the onsite inspection weeks.

The inspection team will examine the returned documentation from the first RFI and identify/select specific systems and equipment (e.g., CSs/CDAs) 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 July 29, 2022, which will identify the specific systems and equipment that will be utilized to evaluate the CSs/CDAs, defensive architecture, and the areas of the licensee's CSP selected for the cyber security inspection. We request that the additional information provided from the second RFI be made available to the regional office prior to the inspection by August 26, 2022.

SUSQUEHANNA STEAM ELECTRIC STATION, UNITS 1 AND 2 CYBER SECURITY INSPECTION DOCUMENT REQUEST

The required Table RFI #1 information shall be provided on an online repository (preferred) or digital media (CD/DVD) to the lead inspector by June 24, 2022. 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 call the inspection team leader as soon as possible.

Table RFI #1		
Section 3, Paragraph Number/Title:		**IP Ref**
1	A list of all Identified Critical Systems and Critical Digital Assets – highlight/note any additions, deletions or 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 of the Cyber Security Program	03.01(b)
6	Vulnerability screening/assessment and scan program documentation	03.01(c)
7	Cyber Security Incident response documentation, including incident detection, response, and recovery documentation as well as contingency plan development and implementation, including any program documentation that requires testing of security boundary device functionality	03.02(a) and 03.04(b)
8	Device Access and Key Control documentation	03.02(c)
9	Password/Authenticator documentation	03.02(c)
10	User Account/Credential documentation	03.02(d)
11	Portable Media and Mobile Device control documentation, including kiosk security control assessment/documentation	03.02(e)
12	Design change/modification program documentation and a list of all design changes that affected CDAs that have actually been installed and completed since the last cyber security inspection, including either a summary of the design change or the 50.59 documentation of the change.	03.03(a)
13	Supply Chain Management documentation including any security impact analysis for new acquisitions	03.03(a), (b) and (c)
14	Configuration Management documentation including any security impact analysis performed due to configuration changes since the last inspection	03.03(a) and (b)
15	Cyber Security Plan and any 50.54(p) analysis to support changes to the plan since the last inspection	03.04(a)
16	Cyber Security Metrics tracked (if applicable)	03.06 (b)
17	Provide documentation describing any cyber security changes to the access authorization program since the last cyber security inspection.	Overall
18	Provide a list of all procedures and policies provided to the NRC with their descriptive name and associated number (if available)	Overall
19	Performance testing report (if applicable)	03.06 (a)

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 July 29, 2022, 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 July 29, 2022, 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 cyber security inspection. The additional information requested for the specific systems and equipment is identified in Table RFI #2.

The Table RFI #2 information shall be provided to the lead inspector by August 26, 2022. The preferred file format for all lists is a searchable Excel spreadsheet. The information should be indexed and hyper-linked to facilitate ease of use. If you have any questions regarding this information, please call the inspection team leader as soon as possible.

Table RFI #2		
Section 3, Paragraph Number/Title:		**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)
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 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 data sheets 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	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	03.05
13	For the selected systems, provide design change/modification packages including completed work orders since the last cyber security inspection	03.03(a)

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 1ST Week Onsite) to the team by October 3, 2022, the first day of the inspection.

Table 1ST Week Onsite		
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(b)
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	03.05

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. UFSAR, if not previously provided;

b. Original SER and Supplements;

c. Quality Assurance Plan;

d. Technical specifications, if not previously provided; and

e. Latest IPE/PRA Report.

(2) Vendor Manuals, Assessment 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 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.