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

May 15, 2018

Mr. Timothy S. Rausch
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 INSPECTION
NOTIFICATION TO PERFORM INSPECTION 05000387/2018403 AND
05000388/2018403

Dear Mr. Rausch:

On October 15, 2018, the U.S. Nuclear Regulatory Commission (NRC) will begin a team inspection in accordance with Inspection Procedure (IP) 71130.10P "Cyber-Security," issued May 15, 2017 at your Susquehanna Steam Electric Station, Units 1 and 2 (Susquehanna). The inspection will be performed to evaluate and verify your ability to meet full implementation requirements of the NRC's Cyber-Security Rule, Title 10, *Code of Federal Regulations* (CFR), Part 73, Section 54, "Protection of Digital Computer and Communication Systems and Networks." The onsite portion of the inspection will take place during the weeks of October 15-19, 2018, and October 29 – November 2, 2018. Experience has shown that team 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 the cyber security Inspection Procedure. This information should be made available via compact disc and delivered to the regional office no later than July 23, 2018. The inspection team will review this information and, by August 20, 2018, 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 your plant'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 September 17, 2018.

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 15, 2018.

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 Jigar Patel. We understand that our regulatory contact for this inspection is Mr. Charlie Manges of your organization. If there are any questions about the inspection or the material requested, please contact the lead inspector at 610-337-5188 or via e-mail at Jigar.Patel1@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.

This letter and its enclosure will be available for public inspection and copying at http://www.nrc.gov/reading-rm/adams.html and at the NRC's Public Document Room in accordance with 10 CFR 2.390, "Public Inspections, Exemptions, Requests for Withholding."

Sincerely,

/RA/

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

Docket Nos. 50-387 and 50-388
License Nos. NPF-14 and NPF-22

Enclosure:
Susquehanna Steam Electric Station
Cyber Security Inspection Document Request

cc w/encl:
Distribution via ListServ

SUBJECT: SUSQUEHANNA STEAM ELECTRIC STATION, UNITS 1 AND 2 INFORMATION REQUEST FOR THE CYBER-SECURITY INSPECTION NOTIFICATION TO PERFORM INSPECTION 05000387/2018403 AND 05000388/2018403 DATED MAY 15, 2018

Distribution: (via e-mail)
DLew, RA
DCollins, DRA
MGray, DRP
DPelton, DRP
MFerdas, DRP
JYerokun, DRS
BWelling, DRS
JKrafty, BC
SBarber, DRP
ATurilin, DRP
LMicewski, SRI
TDaun, DRP, RI
JPatel, DRS
GDentel, DRS
AGould, DRP, AA
JBowen, RI, OEDO
RidsNrrPMSusquehanna Resource
RidsNrrDorlLpl1 Resource
ROPreports Resource

DOCUMENT NAME: G:\DRS\Engineering Branch 2\Patel J\Cyber Security Inspection\RFI\Susquehanna_CyberFI_120d RFI Letter.docx
ADAMS ACCESSION NUMBER: ML18136A614

☑ SUNSI Review		☑ Non-Sensitive ☐ Sensitive		☑ Publicly Available ☐ Non-Publicly Available	
OFFICE	RI/DRS	RI/DRS			
NAME	JPatel	GDentel			
DATE	05/14/18	05/15/18			

OFFICIAL RECORD COPY

SUSQUEHANNA STEAM ELECTRIC STATION
CYBER-SECURITY INSPECTION DOCUMENT REQUEST

Inspection Report:	05000387/2018403 and 05000388/2018403
Inspection Dates:	October 15 – 19, 2018 and October 29 – November 2, 2018
Inspection Procedure:	IP 71130.10P, "Cyber-Security," Issue Date May 15, 2017
Reference:	Guidance Document for Development of the Request for Information (RFI) and Notification Letter for Full-Implementation of the Cyber Security Inspection, Issue Date October 26, 2017

NRC Inspectors:	Jigar Patel, Lead 610-337-5188 Jigar.Patel1@nrc.gov	Louis Dumont 610-337-5183 Louis.Dumont@nrc.gov
NRC Contractors:	Alan Konkal Alan.Konkal@nrc.gov	Timothy Wright Timothy.Wright@nrc.gov
NRC Observers:	Catherine Allen 301-287-3620 Catherine.Allen@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 IP. 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 July 23, 2018, or sooner, to facilitate the selection of the specific items that will be reviewed during the onsite inspection weeks. All requests for information shall follow the Table RFI #1 and the guidance document referenced above.

The required Table RFI #1 information shall be provided on compact disc (CD) to the lead inspector by July 23, 2018. Please provide four copies of each CD submitted (i.e., one for each inspector/contractor). The preferred file format for all lists is a searchable Excel spreadsheet file on a CD. These CDs 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.

SUSQUEHANNA STEAM ELECTRIC STATION
CYBER-SECURITY INSPECTION DOCUMENT REQUEST

Table RFI #1		
Reference Section 3, Paragraph Number/Title:		Items
1	List All Identified Critical Systems and Critical Digital Assets	All
2	List CDA Facility and Site Ethernet – Transmission Control Protocol/Internet Protocol (TCP/IP) Based Local Area Networks (LANs) and Identify Those LAN's That Have Non-CDAs On Them	All
3	List CDA Facility and Site Non-Ethernet TCP/IP Based LANs Including Those Industrial Networks and Identify LANs That Have Non-CDAs On Them	All
4	Network Topology Diagrams (Be Sure To Include all Network Intrusion Detection Systems (NIDS) and Security Information and Event Management (SIEMs) for Emergency Preparedness (EP) networks and Security Level 3 and 4 Networks)	All
8	List All Network Security Boundary Devices for EP Networks and All Network Security Boundary Devices for Levels 3 and 4	All
9	List CDA Wireless Industrial Networks	All
11	NIDS Documentation for Critical Systems That Have CDAs Associated with Them	11.a.1) 11.a.2)
12	SIEM Documentation for Critical systems That Have CDAs Associated with Them	12.a.1) 12.a.2)
14	List EP and Security Onsite and Offsite Digital Communication Systems	All
25	Cyber Security Assessment and Cyber Security Incident Response Teams	All

In addition to the above information please provide the following:

(1) Electronic copy of your current Cyber Security Plan

(2) Electronic copy of summary of changes (if any), including any 10 CFR 50.54p analysis to support those changes, made to the originally approved Cyber Security Plan

(3) Electronic copy of a matrix that summarizes what controls are in place to satisfy the controls required by Policies and Procedures

(4) Electronic copy of the Updated Final Safety Analysis Report and technical specifications

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

(6) Current management and engineering organizational charts

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 (i.e., Table RFI #2). The inspection team will submit the specific systems and equipment list to your staff by August 20, 2018, 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.

SUSQUEHANNA STEAM ELECTRIC STATION
CYBER-SECURITY INSPECTION DOCUMENT REQUEST

II. Additional Information Requested to be Available Prior to Inspection

As stated above, in Section I. of this enclosure, 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 August 20, 2018 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 your station's CSP selected for the cyber-security inspection. The additional information requested for the specific systems and equipment is identified in Table RFI #2. All requested information shall follow the Table RFI #2 and the guidance document referenced above.

The Table RFI #2 information shall be provided on CD to the lead inspector by September 17, 2018. Please provide four copies of each CD submitted (i.e., one for each inspector/contractor). The preferred file format for all lists is a searchable Excel spreadsheet file on a CD. These CDs 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
5	Plant Computer System Block Diagram (If Plant Computer System Is Selected for Inspection)	All
6	Plant Security System Block Diagram (If Security Computer System Is Selected for Inspection)	All
7	Systems That Are Distributed Block Diagrams (For Systems Selected For Inspection)	All
10	Host-Based Intrusion Detection System Documentation (For CDAs for Systems Selected for Inspection)	10.a.1) 10.a.2)
13	List all Maintenance and Test Equipment Used On CDAs for Systems Selected for Inspection	All
15	Configuration Management	All
16	Supply Chain Management	16.b. 16.c.1) 16.c.5) 16.c.6)
17	Portable Media and Mobile Device Control	All
18	Software Management	All
20	Vendor Access and Monitoring	All
21	Work Control	All
22	Device Access and Key Control	All
23	Password/Authenticator Policy	All
24	User Account/Credential Policy	All
26	Corrective Actions Since Last NRC Inspection	All

In addition to the above information please provide the following:

- The documented CSP assessment and analysis for each CDA in each of the selected systems

SUSQUEHANNA STEAM ELECTRIC STATION
CYBER-SECURITY INSPECTION DOCUMENT REQUEST

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

For the specific systems and equipment identified in this enclosure's Section II., provide the following RFI (i.e., Table 1ST Week Onsite) on a CD by October 15, 2018, the first day of the inspection. All requested information shall follow the Table 1ST Week Onsite and the guidance document referenced above.

Please provide four copies of each CD submitted (i.e., one for each inspector/contractor). The preferred file format for all lists is a searchable Excel spreadsheet file on a CD. These CDs 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 1ST Week Onsite		
Section 3, Paragraph Number/Title:`		Items
10	Host-Based Intrusion Detection System Documentation for CDAs for systems selected for inspection	10.a.3) thru 10.a.12)
11	NIDS Documentation for Critical Systems That Have CDAs Associated with Them	11.a.3) thru 11.a.15)
12	SIEM Documentation for Critical Systems That Have CDAs Associated with Them	12.a.3) thru 12.a.14)
16	Supply Chain Management	16.c.2) 16.c.3) 16.c.4)
19	Cyber Security Event Notifications	All

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. Original Final Safety Analysis Report Volumes;
b. Original Safety Evaluation Report and Supplements;
c. Final Safety Analysis Report Question and Answers;
d. Quality Assurance (QA) Plan;
e. Latest Individual Plant Examination for External Events/Probabilistic Risk Assessment Report; and
f. Vendor Manuals

(2) Assessment and Corrective Actions:

a. The most recent Cyber Security 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.

SUSQUEHANNA STEAM ELECTRIC STATION
CYBER-SECURITY INSPECTION DOCUMENT REQUEST

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.