UNITED STATES
NUCLEAR REGULATORY COMMISSION
REGION I
2100 RENAISSANCE BLVD., Suite 100
KING OF PRUSSIA, PA 19406-2713

September 28, 2017

Mr. Richard Bologna
Site Vice President
First Energy Nuclear Operating Company
Beaver Valley Power Station
P. O. Box 4
Shippingport, PA 15077-0004

SUBJECT: BEAVER VALLEY POWER STATION UNITS 1 AND 2 - INFORMATION REQUEST FOR THE "CYBER-SECURITY" BASELINE INSPECTION NOTIFICATION TO PERFORM INSPECTION 05000334/2018403 AND 05000412/2018403

Dear Mr. Bologna:

On January 29, 2018, the U.S. Nuclear Regulatory Commission (NRC) will begin a baseline inspection in accordance with Inspection Procedure (IP) 71130.10 "Cyber-Security," issued May 15, 2017 at the Beaver Valley Power Station, Units 1 and 2. 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 January 29-February 2, 2018, and February 12-16, 2018. 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 the cyber-security Inspection Procedure. This information should be made available via compact disc and delivered to the regional office no later than October 31, 2017. The inspection team will review this information and, by November 17, 2017, 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 station'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 December 11, 2017.

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, January 29, 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 Mr. David Werkheiser. We understand that our regulatory contact for this inspection is Mr. David Wacker of your organization. If there are any questions about the inspection or the material requested, please contact the lead inspector at 610-337-5316 or via e-mail at David.Werkheiser@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. 50-334 and 50-412
License Nos. DPR-66 and NPF-73

Enclosure:
Beaver Valley Power Station, Units 1 and 2
Cyber-Security Inspection Document Request

cc w/encl: Distribution via ListServ

SUBJECT: BEAVER VALLEY POWER STATION UNITS 1 AND 2 – INFORMATION REQUEST FOR THE "CYBER-SECURITY" BASELINE INSPECTION NOTIFICATION TO PERFORM INSPECTION 05000334/2018403 AND 05000412/2018403 DATED SEPTEMBER 28, 2017

DISTRIBUTION w/encl:
DDorman, RA
DLew, DRA
RLorson, DRP
DPelton, DRP
JYerokun, DRS
BWelling, DRS
SHorvitz, DRP
SKennedy, DRP
SShaffer, DRP
CSafouri, DRP
JKrafty, DRP, SRI
DWerkheiser, DRS
GDentel, DRS
CBozlinski, DRP, ROAA
JBowen, RI, OEDO
RidsNrrPMBeaverValley Resource
RidsNrrDorlLpl1 Resource
ROPreports Resource

DOCUMENT NAME: G:\DRS\Engineering Branch 2\Branch Cyber Security\Cyber 120-Day Letters\BV-CyberFI_120d RFI Letter.docx ADAMS ACCESSION NUMBER: ML17271A066

☑ SUNSI Review		☑ Non-Sensitive ☐ Sensitive		☑ Publicly Available ☐ Non-Publicly Available	
OFFICE	RI DRS	RI DRS			
NAME	DWerkheiser/DW	GDentel/GD			
DATE	09/28/17	09/28/17			

OFFICIAL RECORD COPY

BEAVER VALLEY POWER STATION
CYBER-SECURITY INSPECTION DOCUMENT REQUEST

Inspection Report:	05000334/2018403 and 05000412/2018403
Inspection Dates:	January 29 - February 2, 2018 and February 12 - 16, 2018
Inspection Procedure:	IP 71130.10, "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 May 25, 2017

NRC Inspectors:	David Werkheiser, Lead (610) 337-5316 David.Werkheiser@nrc.gov	Jeff Rady (610) 337-5380 Jeff.Rady@nrc.gov
NRC Contractors:	John Walley (301) 287-3717 John.Walley@nrc.gov	Frederick Priester (301) 230-4590 Frederick.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 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 October 31, 2017, 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 November 17, 2017, 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 December 11, 2017. 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 October 31, 2017. Please provide four copies of each CD submitted (i.e., one for each inspector/contactor). 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 #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 LANs 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.

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 November 17, 2017, for the second RFI (i.e., Table RFI #2).

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 November 17, 2017, 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.

BEAVER VALLEY POWER STATION
CYBER-SECURITY INSPECTION DOCUMENT REQUEST

The Table RFI #2 information shall be provided on CD to the lead inspector by December 11, 2017. Please provide four copies of each CD submitted (i.e., one for each inspector/contactor). 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.a.) 16.b.1) 16.b.5) 16.b.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.

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 January 29, 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/contactor). 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.b.2) 16.b.3) 16.b.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.

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.