UNITED STATES
NUCLEAR REGULATORY COMMISSION
REGION II
245 PEACHTREE CENTER AVENUE NE, SUITE 1200
ATLANTA, GEORGIA 30303-1257

January 23, 2020

Ernest J. Kapopoulos, Jr.
Site Vice President
H.B. Robinson Steam Electric Plant
Duke Energy Progress, LLC
3581 West Entrance Road, RNPA01
Hartsville, SC 29550

SUBJECT: H.B. ROBINSON STEAM ELECTRIC PLANT UNIT 2 - INFORMATION REQUEST FOR THE CYBER-SECURITY BASELINE SECURITY INSPECTION, NOTIFICATION TO PERFORM INSPECTION 05000261/2020402

Dear Mr. Kapopoulos:

On May 18, 2020, the U.S. Nuclear Regulatory Commission (NRC) will begin a baseline inspection at your H.B. Robinson Steam Electric Plant, Unit 2. The inspection will be conducted in accordance with Inspection Procedure (IP) 71130.10P "Cyber-Security," dated May 15, 2017. The inspection will be performed to evaluate and verify your ability to meet the Milestone 8 (i.e., 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 May 18, 2020, and June 8, 2020.

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 IP. This information should be made available via secure site (i.e., Sharepoint, Certrec) no later than March 16, 2020. The inspection team will review this information and, by March 30, 2020, 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 site's cyber security program selected for the inspection. This information should be made available via secure site (i.e., Sharepoint, Certrec) no later than April 27, 2020.

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, May 18, 2020. 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. Ellery Coffman. We understand that our regulatory contact for this inspection is Mr. Jeffrey Remick of your organization. If there are any questions about the inspection or the material requested, please contact the lead inspector at 404-997-4633 or via e-mail at ellery.coffman@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, under 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 made available for public inspection and copying at http://www.nrc.gov/reading-rm/adams.html and at the NRC Public Document Room in accordance with 10 CFR 2.390, "Public Inspections, Exemptions, Requests for Withholding."

Sincerely,

/RA/

Scott M. Shaeffer, Chief
Engineering Branch 2
Division of Reactor Safety

Docket Nos. 50-261
License Nos. DPR-23

Enclosure:
Security Inspection Document Request

cc w/encl: Distribution via ListServ

SUBJECT: H.B. ROBINSON STEAM ELECTRIC PLANT UNIT 2 - INFORMATION REQUEST FOR THE CYBER-SECURITY BASELINE SECURITY INSPECTION, NOTIFICATION TO PERFORM INSPECTION 05000261/2020402 DATED JANUARY 23, 2020

DISTRIBUTION:
A. Prada, OCIO
T. Marshall, NSIR
E. Coffman, RII
J. Montgomery, RII

ADAMS ACCESSION NUMBER: ML20024E506

OFFICE	RII/DRS	RII/DRS
NAME	ECoffman	SShaeffer
DATE	1/21/2020	1/23/2020

OFFICIAL RECORD COPY

Inspection Report:	05000261/2020402
Inspection Dates:	May 18, 2020, and June 8, 2020
Inspection Procedure:	IP 71130.10P "Cyber-Security," dated May 15, 2017
Reference:	ML17156A215, "Guidance Document for Development of the Request for Information (RFI) and Notification Letter for Full-Implementation of the Cyber-Security Inspection," Revision 0

NRC Inspectors:	Ellery Coffman, Lead 404-997-4633 ellery.coffman@nrc.gov	Jonathan Montgomery 404-997-4638 jonathan.montgomery@nrc.gov
NRC Contractors:	Tim Marshall tim.marshall@nrc.gov	Alexander Prada alexander.prada@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 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 by March 16, 2020, 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 March 30, 2020, 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 by April 27, 2020. All requests for information shall follow the guidance document ML17156A215 referenced above.

The required Table RFI 1 information shall be provided via secure site (i.e., Sharepoint, Certrec) by March 16, 2020. The preferred file format for all lists is object character recognition (OCR) readable or a searchable Excel spreadsheet file. These files 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:		**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-CDA's 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-CDA's on them	All
4	Network Topology Diagrams (be sure to include all NIDS and SIEMs for 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	Network intrusion detection system documentation for Critical Systems that have CDAs associated with them	11.a.1) 11.a.2)
12	Security Information and Event Management (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
28	Copy of Current Cyber Security Plan and copy of any 50.54(p) analysis to support changes to the plan	All

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.

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 March 30, 2020 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 March 30, 2020 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. All requested information shall follow the guidance document ML17156A215 referenced above.

The Table RFI 2 information shall be provided on secure site (i.e., Sharepoint or Certrec) by April 27, 2020. The preferred file format for all lists is object character recognition (OCR) readable or a searchable Excel spreadsheet file. These files 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 (M&TE) 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
27	Cyber-Security Assessments for Selected Systems	All

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) by May 18, 2020, the first day of the inspection. All requested information shall follow the guidance document ML17156A215 referenced above.

The preferred file format for all lists is object character recognition (OCR) readable or a searchable Excel spreadsheet file. These files 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	Network Intrusion Detection System Documentation for Critical Systems that have CDAs associated with them	11.a.3) thru 11.a.15)
12	Security Information and Event Management (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. Updated Final Safety Analysis Report, if not previously provided;
   b. Original FSAR Volumes;
   c. Original SER and Supplements;
   d. FSAR Question and Answers;
   e. Quality Assurance Plan;
   f. Technical Specifications, if not previously provided;
   g. Latest IPE/PRA Report; and
   h. Vendor Manuals, for applicable systems selected

(2) Assessment and Corrective Actions:
   a. The most recent Cyber-Security Quality Assurance (QA) audit and/or self-assessment; and
   b. The last 73.55(m) assessment performed; and
   c. Corrective action documents (e.g., condition reports, including status of corrective actions) generate 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.

PAPERWORK REDUCTION ACT STATEMENT

This letter contains voluntary 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 (approval number 3150–0011). The burden to the public for these information collections is estimated to average 60 hours per response. Send comments regarding this information collection to the Information Services Branch, Office of the Chief Information Officer, Mail Stop: O-1F13, U.S. Nuclear Regulatory Commission, Washington, DC 20555-0001, or by e-mail to Infocollects.Resource@nrc.gov, and to the Desk Officer, Office of Information and Regulatory Affairs, NEOB-10202, (3150-0011) Office of Management and Budget, Washington, DC 20503.

Public Protection Notification

The NRC may not conduct nor 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 OMB control number.