UNITED STATES
NUCLEAR REGULATORY COMMISSION
REGION II
245 PEACHTREE CENTER AVENUE N.E., SUITE 1200
ATLANTA, GEORGIA 30303-1200

June 29, 2025

Laura A. Basta
Site Vice President
H. B. Robinson Steam Electric Plant
Duke Energy Progress, LLC
3581 West Entrance Road, RNPA11
Hartsville, SC 29550

SUBJECT: H. B. ROBINSON STEAM ELECTRIC PLANT, UNIT 2 – NOTIFICATION OF CYBER SECURITY INSPECTION AND REQUEST FOR INFORMATION (NRC INSPECTION REPORT 05000261/2025403)

Dear Laura A. Basta:

On September 8, 2025, the U.S. Nuclear Regulatory Commission (NRC) will begin a baseline inspection in accordance with Inspection Procedure (IP) 71130.10 “Cyber-Security,” Revision 0 at your H. B. Robinson Steam Electric Plant, Unit 2. The inspection will be performed to evaluate and verify your ability to provide assurance that your digital computer and communication systems and networks associated with safety, security, or emergency preparedness (SSEP) functions are adequately protected against cyber-attacks in accordance with the requirements of Title 10, *Code of Federal Regulations* (CFR), Part 73, Section 54, and the NRC approved Cyber Security Plan (CSP). The onsite portion of the inspection will take place during the week of September 8, 2025.

Experience has shown that baseline inspections are extremely resource intensive, both for the NRC inspectors and the licensee staff. 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 electronically no later than **July 25, 2025**. The inspection team will review this information and, by **August 1, 2025**, 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 CSP selected for the cyber-security inspection. This information will be requested for review in the regional office prior to the inspection by **September 1, 2025**.

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, **September 8, 2025**.

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 Larry J. Jones Jr. If there are any questions about the inspection or the material requested, please contact the lead inspector at 404-997-4837 or via e-mail at Larry.Jones@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,

Daniel M. Bacon Signed by Bacon, Daniel
on 06/29/25

Daniel Bacon, Branch Chief
Engineering Branch 2
Division of Operating Reactor Safety

Docket No.: 50-261
License No.: DPR-23

Enclosure:

H.B. Robinson Steam Electric Plant Unit 2 Cyber-Security Inspection Document Request

cc w/encl: Distribution via LISTSERV

SUBJECT: H. B. ROBINSON STEAM ELECTRIC PLANT, UNIT 2 – NOTIFICATION OF CYBER SECURITY INSPECTION AND REQUEST FOR INFORMATION (NRC INSPECTION REPORT 05000261/2025403) DATED JUNE 29, 2025

DISTRIBUTION:
D. Bacon, RII/DORS/EB2
L. Jones, RII/DORS/EB1
J. Alamudun, RII/DORS/EB2
M. Fannon, RII/DORS/RPB2
J. Zeiler, RII/DORS/RPB2
M. Fernandez, NSIR/CSB

ADAMS ACCESSION NUMBER: ML25178A309

X SUNSI Review		X Non-Sensitive □ Sensitive		X Publicly Available □ Non-Publicly Available	
OFFICE	RII/DORS/EB2	RII/DORS/EB2	RII/DORS/EB1		
NAME	J. Alamudun	L. Jones	D. Bacon		
DATE	6/27/2025	6/27/2025	6/29/2025		

OFFICIAL RECORD COPY

Inspection Report:	05000261/2025403	
Inspection Dates:	September 8 - 12, 2025	
Inspection Procedure:	IP 71130.10, “Cyber-Security,” Revision 0	
NRC Inspectors:	Larry J. Jones Jr., Lead 404-997-4837 Larry.Jones@nrc.gov	Folajimi (Jimi) Alamudun 404-997-4490 Folajimi.Alamudun@nrc.gov
NRC Contractors:	James Hartman James.hartman@nrc.gov	Trace Coleman trace.coleman@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 to the regional office by **July 25, 2025** or sooner, to facilitate the selection of the specific items that will be reviewed during the onsite inspection week.

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 **August 1, 2025**, 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 **September 1, 2025**.

The required Table RFI 1 information shall be provided electronically to the lead inspector by **July 25, 2025**. The preferred file format for all lists is 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		
Request:		**IP Ref**
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	Network Topology Diagrams to include information and data flow for critical systems in levels 2, 3, and 4 (If available)	Overall
3	The most recent effectiveness analysis and self-assessment(s) of the Cyber Security Program.	03.01(b)
4	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)
5	Design change/ modification program documentation and a list of all design changes completed since the last cyber security inspection, including either a summary of the design change or the 50.59 documentation for the change.	03.03(a)
6	Configuration Management documentation including any security impact analysis performed due to configuration changes since the last inspection	03.03(a) and (b)
7	Cyber Security Plan and any 50.54(p) analysis to support changes to the plan since the last cyber inspection.	03.04(a)
8	Provide a list of all cybersecurity procedures and policies with their descriptive name and associated number.	Overall
9	Cyber Security Performance Metrics tracked (if applicable).	03.06(b)
10	Performance testing report (if applicable).	03.06(a)

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 **August 1, 2025,** for the second RFI (i.e., RFI #2).

II. ***<u>Additional Information Requested to be Available Prior to Inspection.</u>***

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 **August 1, 2025**, 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 electronically to the lead inspector by **September 1, 2025.** The preferred file format for all lists is 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

Request:		**Items**
	For the Critical Systems / CDAs chosen for inspection provide:	
1	Ongoing Monitoring and Assessment (OM&A) activity performed on the selected inspection samples' Critical Systems.	03.01(a)
2	All Security Control Assessments for the selected design changes and Critical System selected CDAs.	03.01(a)
3	Copy of vulnerability management program documentation. All vulnerability screenings and assessments completed prior to placing new CDA equipment into service as part of the selected design changes.	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) for the systems 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 critical systems.	03.02(c)
6	Copies of all periodic reviews of the access authorization list for the selected systems since the last inspection. Provide documentation describing any cyber security changes to the access authorization program (AAP) since the last cyber security inspection.	03.02(d)
7	Baseline configuration data sheets for the selected CDAs.	03.03(a)
8	Copies of the purchase order documentation for any new equipment purchased for the selected Critical Systems and design changes.	03.03(c)

9	Copies of any cyber security drills performed since the last inspection, along with any reports or assessments generated.	03.02(a)
10	Vulnerability Management program screening and assessment policies and procedures.	03.01(c)
11	Portable Media and Mobile Device (PMMD) control documentation, including kiosk security control assessment/documentation.	03.02(e)
12	Device Access and Key Control program documentation.	03.02(c)
13	The most recent Cybersecurity Quality Assurance audit and/or self-assessment and a list of Corrective Actions generated as a result.	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 Week Onsite) electronically by **September 8, 2025**.

Table: Week Onsite		
Request:		**Items**
1	Any cyber security event reports submitted in accordance with 10 CFR 73.77 since the last cyber security inspection.	03.04(a)

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 during daily de-brief meetings).