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

June 27, 2023

Sonny Dean
Site Vice President
Southern Nuclear Operating Co., Inc.
Edwin I. Hatch Nuclear Plant
11028 Hatch Parkway North
Baxley, GA 31513

SUBJECT: EDWIN I. HATCH NUCLEAR PLANT UNITS 1 & 2 - INFORMATION REQUEST FOR THE "CYBER-SECURITY" BASELINE INSPECTION, NOTIFICATION TO PERFORM INSPECTION 05000321/2023403 AND 05000366/2023403

Dear Sonny Dean:

On October 02, 2023, 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 Hatch Nuclear Plant Units 1 & 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 Title 10 of the Code of Federal Regulations (10 CFR) 73.54 and the U.S. Nuclear Regulatory Commission (NRC) approved cyber security plan (CSP). The onsite portion of the inspection will take place during the week of October 02, 2023.

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 28, 2023**. The inspection team will review this information and, by **August 4, 2023**, will request the specific items that should be provided for review. This 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. We request that the information provided from the second RFI be made available to the regional office prior to the inspection by **September 8, 2023**.

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 02, 2023**.

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 William Monk. We understand that our regulatory contacts for this inspection are Scott Junkin and Jimmy Collins, Licensing Managers of your organization. If there are any questions about the inspection or the material requested, please contact the lead inspector at (404) 997-4579 or via e-mail at william.monk@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 06/27/23

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

Docket Nos. 50-321; 50-366

License Nos. DPR-57; NPF-5

Enclosure:
Edwin I. Hatch Nuclear Plant Units 1 & 2 Cyber-Security Inspection Document Request

cc w/encl: Distribution via LISTSERV

SUBJECT: EDWIN I. HATCH NUCLEAR PLANT UNITS 1 & 2 - INFORMATION REQUEST FOR THE “CYBER-SECURITY” BASELINE INSPECTION, NOTIFICATION TO PERFORM INSPECTION 05000321/2023403 AND 05000366/2023403 DATED JUNE 27, 2023

DISTRIBUTION:
W. Monk, RII
D. Bacon, RII
J. Montgomery, RII
A. Blamey, RII
R. Smith, RII
M. Fernandez, NSIR
R2EICS
PUBLIC

ADAMS ACCESSION NUMBER: ML23178A001

X SUNSI Review		X Non-Sensitive ☐ Sensitive		X Publicly Available ☐ Non-Publicly Available	
OFFICE	RII/DRS	RII/DRS	RII/DRS		
NAME	W. Monk	J. Montgomery	D. Bacon		
DATE	06/272023	06/272023	06/27/2023		

OFFICIAL RECORD COPY

H. B. ROBINSON STEAM ELECTRIC PLANT UNIT 2
CYBER-SECURITY INSPECTION DOCUMENT REQUEST

Inspection Report:	05000321/2023-403 and 05000366/2023-403
Inspection Dates:	October 02 – 06, 2023
Inspection Procedure:	IP 71130.10, "Cyber-Security," Revision 0 (Effective: 01/01/2022)
Reference:	"Guidance Document for Development of the Request for Information (RFI) and Notification Letter for Full-Implementation of the Cyber-Security Inspection," Rev. 2 (Issued: 11/22/2021)

NRC Inspectors:	William Monk, Lead 404-909-4579 william.monk@nrc.gov	Jonathan Montgomery 404-997-4880 jonathan.montgomery@nrc.gov
NRC Contractors:	Al Konkal 561-989-0210 *alan.konkal@nrc.gov*	Michael Shock 301-415-7000 michael.shock@nrc.gov

I. Information Requested for In-Office Preparation

The initial request for information (i.e., RFI #1) 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. RFI #1 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. RFI #1's requested information is specified below in Table: RFI #1 and requested to be provided electronically to the inspection team by **July 28, 2023**, 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 RFI #1 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 4, 2023**, 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 RFI #2 be made available to the inspection team by **September 8, 2023**. All requests for information shall follow the guidance document U.S. NRC - Guidance Document for Development of the Request for Information (RFI) and Notification Letter for Full Implementation of the Cyber-Security Inspection, referenced above.

The required Table: RFI #1 information shall be provided electronically to the lead inspector by **July 28, 2023**. 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		
Paragraph Number/Title:		**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	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 (OM&A) program documentation.	03.01(a)
5	The most recent effectiveness analysis and self-assessments of the Cyber Security Program.	03.01(b)
6	Password/Authenticator program documentation.	03.02(c)
7	Design change/ modification program documentation and a list, with descriptions, of all design changes that affected CDAs that have actually been installed and completed since the last two cyber security inspections, including either a summary of the design change or the 50.59 documentation for the change.	03.03(a)
8	Supply Chain Management program documentation, including any security impact analysis for new acquisitions.	03.03(a), (b) and (c)
9	Cyber Security Plan and any 50.54(p) analysis to support changes to the plan since the last cyber inspection.	03.04(a)
10	Cyber Security Performance Metrics tracked (if applicable).	03.06(b)
11	Provide a list of all procedures and policies provided to the NRC with their descriptive name and associated number (if available).	Overall
12	Performance testing report (if applicable).	03.06(a)
13	Corrective actions taken as a result of cyber security incidents/issues to include previous NRC violations and Licensee Identified Violations since two last cyber security inspections.	03.05

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 **August 4, 2023,** 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 **August 4, 2023,** for the second RFI (i.e., RFI #2). RFI #2 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 and requested information shall follow the guidance document referenced above.

The Table: RFI #2 information shall be provided to the lead inspector by **September 8, 2023**. 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		
Paragraph Number/Title:		**Items**
	For the Critical Systems / CDAs chosen for inspection provide:	
1	Ongoing Monitoring and Assessment activity performed on the selected inspection samples' critical systems.	03.01(a)
2	All Security Control Assessments for the selected critical systems.	03.01(a)
3	All vulnerability screenings/assessments associated with or scans performed on the selected critical systems 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	03.02(b)

Table: RFI #2		
Paragraph Number/Title:		**Items**
	Information and Event Management (SIEM) systems for the critical systems chosen for inspection.	
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 (AA) list for the selected systems since the last cyber 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 critical systems 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 critical systems including documentation of the results the last time the backups were executed.	03.02(a) 03.04(b)
12	Vulnerability screening/assessment and scan program documentation.	03.01(c)
13	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) and 03.04(b)
14	Device Access and Key Control program documentation.	03.02(c)
15	User Account/Credential documentation.	03.02(d)
16	Portable Media and Mobile Device (PMMD) control documentation, including kiosk security control assessment/documentation.	03.02(e)
17	Configuration Management documentation including any security impact analysis performed due to configuration changes since the last cyber inspection.	03.03(a) and (b)

Table: RFI #2		
Paragraph Number/Title:		**Items**
18	Provide documentation describing any cyber security changes to the access authorization program (AAP) since the last cyber security inspection.	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) to the team by **October 02, 2023**, the first day of the inspection. All requested information shall follow the guidance document referenced above.

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: Week Onsite		
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(a)
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. Updated Final Safety Analysis Report (UFSAR), if not previously provided
b. Original FSAR Volumes
c. Original SER and Supplements
d. FSAR Question and Answers
e. Quality Assurance (QA) Plan
f. Technical Specifications, if not previously provided
g. 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 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 during daily de-brief meetings).

If you have any questions regarding the information requested, please contact the inspection team leader.