UNITED STATES
NUCLEAR REGULATORY COMMISSION
REGION IV
1600 EAST LAMAR BOULEVARD
ARLINGTON, TEXAS 76011-4511

January 18, 2024

G T Powell
President and CEO
STP Nuclear Operating Company
P.O. Box 289
Wadsworth, TX 77483

SUBJECT: SOUTH TEXAS PROJECT ELECTRIC GENERATING STATION, UNITS 1 AND 2 - INFORMATION REQUEST FOR THE "CYBER-SECURITY" BASELINE INSPECTION, NOTIFICATION TO PERFORM INSPECTION 05000498/2024404; 05000499/2024404

Dear G. T. Powell:

On May 20, 2024, the U.S. Nuclear Regulatory Commission (NRC) will begin a baseline inspection in accordance with Inspection Procedure (IP) 71130.10 "Cybersecurity," at your South Texas Project. The inspection will be performed to evaluate and verify your ability to meet the 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."

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 inspection procedure. This information should be made available either in an online repository (preferred) or digital media (CD/DVD) and delivered/available to the regional office no later than February 19, 2024. The inspection team will review this information and, by March 25, 2024, will request the specific items that should be provided for review.

The second group of requested documents will assist the inspection team in the evaluation of the critical systems and critical digital assets, defensive architecture, and the areas of your cyber security program selected for review. This information will be requested for review in the regional office prior to the inspection by April 22, 2024, as identified above.

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 20, 2024.

The fourth group of information is necessary to aid the inspection team in tracking issues identified during 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 documents are up to date and complete 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 Greg Pick. We understand that our regulatory contact for this inspection is Stephanie Rodgers of your organization. If there are any questions about the inspection or the material requested, please contact the lead inspector at 817-504-2105 or via e-mail at greg.pick@nrc.gov.

Paperwork Reduction Act Statement

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,

Signed by Pick, Gregory
on 01/18/24

Greg Pick, Senior Reactor Inspector
Engineering Branch 2
Division of Operations and Reactor Safety

Dockets: 50-498; 50-499
Licenses: NPF-76; NPF-80

Enclosure:
South Texas Project – Cyber-Security Inspection Document Request
cc w/encl: Distribution via LISTSERV

SOUTH TEXAS PROJECT ELECTRIC GENERATING STATION, UNITS 1 and 2 – INFORMATION REQUEST FOR THE "CYBER-SECURITY" BASELINE INSPECTION, NOTIFICATION TO PERFORM INSPECTION 05000498/2024404; 05000499/2024404 DATED JANUARY 18, 2024.

DISTRIBUTION:
JMonninger, ORA
JLara, ORA
GMiller, DORS
MHay, DORS
DCylkowski, RC
JHamman, RIV/OEDO
VDricks, ORA
LWilkins, OCA
DGalvin, NRR
AMoreno, RIV/OCA
RAlexander, RSLO
PVossmar, DORS
HFreeman, DORS
SLichvar, DORS
GKolcum, DORS
CStott, DORS
MZiolkowski, RI
DSchroeder, RI
JWorosilo, RII
JClark, NSIR-SPEB
LReyna, DORS
NTaylor, DORS
GDentel, DORS, RI
GMcCoy, DRS, RII
RSkowowski, DRS, RIII
BYip, DPCP, NSIR
TRivera, DPCP, NSIR
KLawson-Jenkins, DPCP, NSIR
TKeene, DSO, NSIR
DJohnson, DSO, NSIR
JRey, DSO, NSIR

ADAMS ACCESSION NUMBER: **ML24016A235**
☒ SUNSI Review: ADAMS: ☐ Non-Publicly Available ☒ Non-Sensitive
Keyword:
By: ☒ Yes ☐ No ☒ Publicly Available ☐ Sensitive NRC-002

OFFICE	RIV:SRI/DORS/EB2			
NAME	GPick			
SIGNATURE	/**RA/**			
DATE	01/18/24			

OFFICIAL RECORD COPY

Inspection Report: 05000498/2024404; 05000499/2024404

Inspection Dates: Week of May 20, 2024

Inspection Procedure: IP 71130.10, "Cybersecurity,"

Reference: ML21330A088, "Guidance Document for Development of the Request for Information (RFI) and Notification Letter for IP 71130.10, 'Cyber-Security Inspection,'" Revision 2

NRC Inspectors:	Greg Pick, Lead 817-504-2105 greg.pick@nrc.gov	Nnaerika Okonkwo 817-200-1114 nnaerika.okonkwo@nrc.gov
NRC Contractors:	Balla Barro balla.barro@nrc.gov	Justin Bowden justin.bowden@nrc.gov

I. Information Requested for In-Office Preparation

This initial request for information (i.e., Table RFI #1) concentrates on providing the inspection team with information necessary to select appropriate components and cyber security program elements to develop a site-specific inspection plan. The first RFI is used to identify the critical digital assets or systems to be chosen as the "sample set" required to be inspected by the cyber-security inspection procedure. Please provide the information requested in Table RFI #1 to the regional office by February 19, 2024, or sooner, to facilitate the selection of the specific items for review.

The inspection team will examine the documentation from the first RFI and select specific systems and equipment 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 25, 2024, which will be utilized to evaluate the equipment, defensive architecture, and the areas of the licensee's cyber security program for review.

Please provide the information requested by the second RFI to the regional office by April 22, 2024. All requests for information shall follow the referenced guidance document. For information requests that have more than ten (10) documents, provide a compressed (i.e., Zip) file of the documents.

The required Table RFI #1 information shall be provided in an online document repository (preferred) or on digital media (CD/DVD) to the lead inspector by February 19, 2024. 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		
Section 3, **Paragraph Number/Title:**		**IP Ref. Items**
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 program documentation	03.01(a)
5	The most recent effectiveness analysis and self-assessments of the Cyber Security Program	03.01(b)
6	Portable Media and Mobile Device control documentation, including kiosk security control assessment/documentation	03.02(e)
7	Design change/modification program documentation and a list of all cyber-related design changes completed since the last two cyber security inspections, including either a summary describing the design change or the 50.59 documentation for the change.	03.03(a)
8	Supply Chain Management 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 inspection	03.04(a)
10	Cyber Security Metrics tracked (if applicable)	03.06 (b)
11	Provide copies of all cybersecurity program related procedures and policies with their descriptive name and associated number (if available)	Overall
12	Performance testing report (if applicable)	03.06 (a)
13	Corrective actions taken because 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., critical systems/critical digital assets) from the information requested by Table RFI #1 and submit a list of specific systems and equipment to your staff by March 25, 2024, 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 25, 2024, for the second RFI (i.e., RFI #2). The second RFI will request additional information required to evaluate the critical systems and critical digital assets, defensive architecture, and the areas of the cyber security program selected for inspection. The additional information requested for the specific systems and equipment is identified in Table RFI #2. All requested information shall follow the referenced guidance document.

The Table RFI #2 information shall be provided in an online document repository (preferred) or on digital media (CD/DVD) to the lead inspector by April 22, 2024. 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		
Section 3, Paragraph Number/Title:		**Items**
	For the system(s) chosen for inspection provide:	
1	Ongoing Monitoring and Assessment activity performed on the system(s)	03.01(a)
2	All Security Control Assessments for the selected system(s)	03.01(a)
3	All vulnerability screenings/assessments associated with, or scans performed on the selected system(s) 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 Information and Event Management (SIEM) systems for system(s) chosen for inspection	03.02(b)

Table RFI #2		
Section 3, Paragraph Number/Title:		**Items**
5	Documentation (including configuration files and rule sets) for intra-security level firewalls and boundary devices used to protect the selected system(s)	03.02(c)
6	Copies of all periodic reviews of the access authorization list for the selected systems since the last inspection	03.02(d)
7	Baseline configuration information for the selected CDAs	03.03(a)
8	Documentation on any changes, including Security Impact Analyses, performed on the selected system(s) 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 system(s) 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 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 documentation	03.02(c)
15	User Account/Credential documentation	03.02(d)
16	Password/Authenticator documentation	03.02(c)
17	Portable Media and Mobile Device control documentation, including kiosk security control assessment/documentation	03.02(e)
18	Configuration Management documentation including any security impact analysis performed due to configuration changes since the last inspection	03.03(a) and (b)

19	Provide documentation describing any cyber security changes to the access authorization program 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 1ST Week Onsite) to the team by May 20, 2024, the first day of the inspection. All requested information shall follow the referenced guidance document.

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 1ST Week Onsite		
Section 3, 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 because 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	03.04(d)

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 if the inspectors have easy and unrestrained access to them.

a. Updated Final Safety Analysis Report, if not previously provided;

b. Original SER and Supplements related to cybersecurity;

c. FSAR Question and Answers related to cybersecurity;

d. Quality Assurance Plan;

e. Technical Specifications, if not previously provided;

(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 because of the most recent Cybersecurity 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 because 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.