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

September 13, 2022

Mr. 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 CYBERSECURITY BASELINE INSPECTION, NOTIFICATION TO PERFORM INSPECTION 05000498/2022401 AND 05000499/2022401

Dear Mr. Powell:

On November 28, 2022, 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 Electric Generating Station, Units 1, and 2. The inspection objectives are to provide assurance that the digital computer and communication systems and networks associated with safety, security, or emergency preparedness (SSEP) functions are adequately protected against cyberattacks in accordance with Title 10 of the Code of Federal Regulations (10 CFR) 73.54 and your approved cybersecurity plan (CSP), and to verify that any CSP changes and reports have been made in accordance with 10 CFR 50.54(p).

Experience has shown that baseline inspections are extremely resource intensive, both for the NRC inspectors and 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 via digital media (CD/DVD) or an online document repository and delivered/available to the regional office no later than October 7, 2022. The inspection team will review this information and, by October 17, 2022, 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 (CSs/CDAs), 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 November 7, 2022, as identified above.

SOUTH TEXAS PROJECT ELECTRIC GENERATING STATION
CYBER-SECURITY INSPECTION DOCUMENT REQUEST

The third group of requested documents consists of additional 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, November 28, 2022.

The fourth group of information aids 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 requested 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 Nnaerika Okonkwo. 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 817-200-1114 or via e-mail at nnaerika.okonkwo@nrc.gov

Paperwork Reduction Act Statement

This letter contains mandatory 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 under approval number 3150-0011. The burden to the public for these information collections is estimated to average 40 hour(s) per response. Send comments regarding this information collection to the FOIA, Library and Information Collection Branch, Office of the Chief Information Officer, Mail Stop: T6-A10M, U.S. Nuclear Regulatory Commission, Washington, DC 20555-0001, or by email to Infocollects.Resource@nrc.gov, and to the Desk Officer, Office of Information and Regulatory Affairs, NEOB-10202, (3150-0011) OMB, Washington, DC 20503.

Public Protection Notification

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 Website at http://www.nrc.gov/reading-rm/adams.html (the Public Electronic Reading Room).

Sincerely,

Signed by Okonkwo, Nnaerika
on 09/15/22

Nnaerika Okonkwo, Reactor Inspector
Engineering Branch 2
Division of Operating Reactor Safety

SOUTH TEXAS PROJECT ELECTRIC GENERATING STATION
CYBER-SECURITY INSPECTION DOCUMENT REQUEST

Docket Nos. 05000498, 05000499,
License Nos. NPF-76; NPF-80

Enclosure:

South Texas Project Electric Generating Station, Units 1 And 2.
Cyber Security Inspection Document Request
cc w/encl: Distribution via LISTSERV®

SOUTH TEXAS PROJECT ELECTRIC GENERATING STATION
CYBER-SECURITY INSPECTION DOCUMENT REQUEST

SOUTH TEXAS PROJECT ELECTRIC GENERATING STATION, UNITS 1, AND 2 - INFORMATION REQUEST FOR THE CYBERSECURITY BASELINE INSPECTION, NOTIFICATION TO PERFORM INSPECTION 05000498/2022401 AND 05000499/2022401 DATED SEPTEMBER 13, 2022

DISTRIBUTION:
SMorris, ORA
JMonninger, ORA
RLantz, DORS
MHay, DORS
DCylkowski, RC
LMcKown, RIV/OEDO
VDricks, ORA
LWilkins, OCA
DGalvin, NRR
AMoreno, RIV/OCA
RAlexander, RSLO
PVossmar, DORS
RDeese, DORS
SLichvar, DORS
GKolcum, DORS
CStott, DORS
LReyna, DORS
R4-DORS-IPAT
R4Enforcement

ADAMS ACCESSION NUMBER: **ML22255A154**

☒SUNSI Review: ADAMS: ☐ Non-Publicly Available and Sensitive
By: NPO ☒ Yes ☐ No ☒ Publicly Available and non-sensitive

OFFICE	DORS/EB2					
NAME	N.Okonkwo					
SIGNATURE	NPO1					
DATE	09/13/22					

OFFICAL RECORD COPY

SOUTH TEXAS PROJECT ELECTRIC GENERATING STATION
CYBER-SECURITY INSPECTION DOCUMENT REQUEST

Inspection Report: 05000498/2022401; 05000499/2022401

Inspection Date(s): Week of *November 28*

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: Nnaerika Okonkwo, Lead
817-200-1114
Nnaerika.okonkwo@nrc.gov

Larry Jones
404-997-4837
larry.jones@nrc.gov

NRC Contractors: *Steven Leigh*
301-*332-8281*
Steven.leigh@nrc.gov

Tim Marshall
703-964-6891
timothy.marshall@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 IP. The first RFI's requested information is specified below in Table RFI #1. Please provide the information requested in Table RFI #1 to the regional office by October 7, 2022, 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 October 17, 2022, 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 November 7, 2022. All requests for information shall follow the guidance document referenced above. For information requests that have more than ten (10) documents, please provide a compressed (i.e., Zip) file of the documents.

SOUTH TEXAS PROJECT ELECTRIC GENERATING STATION
CYBER-SECURITY INSPECTION DOCUMENT REQUEST

The required Table RFI #1 information shall be provided on digital media (CD/DVD)) or an online document repository to the lead inspector by October 7, 2022. Please provide four copies of each media submitted (i.e., one for each inspector/contactor). The preferred file format for all lists is a searchable Excel spreadsheet file. The media (CDs/DVDs) should be indexed and hyperlinked 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 of the Cyber Security Program	03.01(b)
6	Vulnerability screening/assessment and scan program documentation	03.01(c)
7	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)
8	Device Access and Key Control documentation	03.02(d)
9	Password/Authenticator documentation	03.02(d)
10	User Account/Credential documentation	03.02(d)
11	Portable Media and Mobile Device control documentation, including kiosk security control assessment/documentation	03.02(e)
12	Design change/modification program documentation and a list of all cyber-related design changes completed since the last cyber security inspection, including either a summary describing the design change or the 50.59 documentation for the change.	03.03(a)

Enclosure

13	Supply Chain Management documentation including any security impact analysis for new acquisitions	03.03(a), (b) and (c)
14	Configuration Management documentation including any security impact analysis performed due to configuration changes since the last inspection	03.03(a) and (b)
15	Cyber Security Plan and any 50.54(p) analysis to support changes to the plan since the last inspection	03.04(a)
16	Cyber Security Metrics tracked (if applicable)	03.06 (b)
17	Provide documentation describing any cyber security changes to the access authorization program since the last cyber security inspection.	Overall
18	Provide a list of all procedures and policies provided to the NRC with their descriptive name and associated number (if available)	Overall
19	Performance testing report (if applicable)	03.06 (a)

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.

(4) Implementing and program procedures in a single folder.

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 October 17, 2022, 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 October 17, 2022, 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 cybersecurity 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 referenced above.

The Table RFI #2 information shall be provided on digital media (CD/DVD) or an online document repository to the lead inspector by November 7, 2022. Please provide four copies of each media (CD/DVD) submitted (i.e., one for each inspector/contactor). The preferred file format for all lists is a searchable Excel spreadsheet file. The digital media (CDs/DVDs) should be indexed and hyperlinked 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:		**IP Ref. 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)

Enclosure

Table RFI #2		
Section 3, Paragraph Number/Title:		**IP Ref. Items**
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)
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 data sheets 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	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	03.04(d)

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 Onsite Week) on digital media (CD/DVD) or an online document repository by November 28, 2022, the first day of the inspection. All requested information shall follow the guidance document referenced above.

Please provide four copies of each passive digital media (CD/DVD) submitted (i.e., one for each inspector/contactor). The preferred file format for all lists is a searchable Excel spreadsheet file. The digital media (CDs/DVDs) should be indexed and hyperlinked to facilitate ease of use. If you have any questions regarding this information, please call the inspection team leader as soon as possible.

Table Onsite Week		
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)

Table Onsite Week		
Section 3, Paragraph Number/Title:		**Items**
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	03.04(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 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

(2) Vendor Manuals, Assessments 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) 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 leader.

Enclosure