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

June 28, 2022

Mr. Ken Peters, Senior Vice President
and Chief Nuclear Officer
Attention: Regulatory Affairs
Vistra Operations Company LLC
P.O. Box 1002
Glen Rose, TX 76043

SUBJECT: COMANCHE PEAK NUCLEAR POWER PLANT, UNITS 1 AND 2 - INFORMATION REQUEST FOR THE CYBER-SECURITY BASELINE INSPECTION, NOTIFICATION TO PERFORM INSPECTION 05000445/2022401; 05000446/2022401

Dear Mr. Peters,

On October 24, 2022, the U.S. Nuclear Regulatory Commission (NRC) will begin a baseline inspection in accordance with Inspection Procedure (IP) 71130.10, "Cyber-Security," at your Comanche Peak Nuclear Power Plant. The inspection evaluates and verifies 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 via electronic means (e.g., compact disc or other electronic means) and delivered to the regional office no later than August 1, 2022. The inspection team will review this information and, by August 22, 2022, 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, defensive architecture, and the areas of your cyber security program selected for the cyber-security inspection. This information will be requested for review in the regional office prior to the inspection by September 19, 2022.

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 24, 2022.

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 these 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 Jim Barnette at 817-408-0934 (m) or via email james.barnette@luminant.com of your organization. If there are any questions about the inspection or the material requested, please contact the lead inspector Greg Pick at 817-504-2105 (m) or via e-mail at greg.pick@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 (approval number 3150-0011). Send comments regarding this information collection to the Information Services Branch, Office of the Chief Information Officer, Mail Stop: T6 A10M, 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.

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 Title 10 of the *Code of Federal Regulations* (10 CFR) 2.390, "Public Inspections, Exemptions, Requests for Withholding." Your cooperation and support during this inspection will be appreciated.

Sincerely,

Greg Pick Signed by Pick, Gregory
on 06/28/22

Greg A. Pick
Senior Reactor Inspector
Engineering Branch 2
Division of Operating Reactor Safety

Dockets: 50-445; 50-446
Licenses: NPF-87; NPF-89

Enclosure:
Comanche Peak Nuclear Power Plant
Cyber-Security Inspection Document Request

cc w/encl: Distribution via LISTSERV

COMANCHE PEAK NUCLEAR POWER PLANT, UNITS 1 AND 2 - INFORMATION REQUEST FOR THE CYBER-SECURITY BASELINE INSPECTION, NOTIFICATION TO PERFORM INSPECTION 05000445/2022401; 05000446/2022401 – JUNE 28, 2022

DISTRIBUTION:
SMorris, RA
JMonninger, DRA
RLantz, DORS
MHay, DORS
DCylkowski, RC
VDricks, ORA
LWilkins, OCA
ROrlikowski, RIV/OEDO
DGalvin, NRRG
AMoreno, RIV/OCA
RAlexander, RSLO
FRamirez, IPAT
GWerner, DORS
DProulx, DORS
JMelfi, DORS
ASmallwood, DORS
JEllegood, DORS
AAgrawal, IPAT
DDodson, IPAT
RAzua, IPAT
NDay, DORS
LReyna, DORS
LFlores, IPAT
BCorrell, IPAT
R4Enforcement

ADAMS ACCESSION NUMBER: ML22179A303

■SUNSI Review By: GAP	ADAMS: ■ Yes □ No	□ Non-Publicly Available ■ Publicly Available	■Non-Sensitive □ Sensitive	Keyword: NRC-002

OFFICE	DORS/EB2:SRI					
NAME	GPick					
SIGNATURE	Gap					
DATE	6/28/2022					

OFFICIAL RECORD COPY

Inspection Report: 05000445/2022401; 05000446/2022401

Inspection Dates: October 24 – 28, 2022

Inspection Procedure: IP 71130.10, “Cyber-Security,” dated January 1, 2022

Reference: ML21330A088, “Guidance Document for Development of the Request for Information (RFI) and Notification Letter for Full-Implementation of the Cyber-Security Inspection,” Revision 1

NRC Inspectors:

Greg Pick, (Lead) 817-504-2105 greg.pick@nrc.gov	Stella Opara-Ogunmola 301-287-9286 stella.opara@nrc.gov
Marcus Chisolm 817-200-1426 marcus.chisolm@nrc.gov	

NRC Contractors:

Casey Priester frederick.priester@nrc.gov	Alan Konkal alan.konkal@nrc.gov

I. *Information Requested for In-Office Preparation*

The initial request for information (Table RFI#1) provides the team with the general information necessary to select appropriate components and cyber security program elements to develop a site-specific inspection plan. The initial request for information is used to identify the list of critical systems and critical digital assets plus operational and management security control portions of the cyber security program to be chosen as the “sample set” to be inspected. Please provide the information listed in Table RFI#1 to the regional office by August 1, 2022, or sooner, to facilitate the selection of the specific items that will be reviewed.

The team will examine the returned documentation from the initial request for information and select specific critical systems and critical digital assets to provide for a more deliberate, focused second request for information. The team will submit the second request by August 22, 2022, which will identify the critical systems and critical digital assets that will be utilized to evaluate the defensive architecture and the areas of your cyber security program selected for the inspection. We request that the information for the second request be made available for review by September 19, 2022.

All requests for information shall follow the referenced guidance document ADAMS Accession No. ML21330A088. If a secure document management service is utilized, it is recommended that a separate folder be used corresponding to each item listed below. It is recommended that multiple documents within each folder be individually entered and also combined into a ZIP file that is uploaded into the same folder. Documents should be identified by both document number and noun name. Electronic media on compact disc or paper records (hard copy) are also acceptable. 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**
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(c)
9	Password/Authenticator documentation	03.02(c)
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 design changes completed since the last cyber security inspection,	03.03(a)

Table RFI#1

Section 3, **Paragraph Number/Title:**	**IP Ref**
including either a summary of the design change or the 50.59 documentation for the change.	
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

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

As stated in *Section **I*** above, the team will examine the documentation requested from Table RFI#1 and submit the list of critical systems and critical digital assets to your staff by August 22, 2022 (i.e., RFI#2). The additional information requested for the specific systems and equipment is identified in Table RFI#2. Please provide the Table RFI#2 information to the lead inspector by September 19, 2022. 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**
	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)
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 because of cyber security incidents/issues to include previous NRC violations and Licensee Identified Violations since the last cyber security inspection	03.05

III. ***Information Requested to be Available on First Day of Inspection***

For the critical systems and critical digital assets identified in *Section **II***, provide the following request for information (i.e., Table 1ST Week Onsite) to the team by October 24, 2022*,* the first day of the inspection.

Table 1ST Week Onsite		
Section 3, Paragraph Number/Title:		**IP Ref**
1	Any cyber security event reports submitted in accordance with 10 CFR 73.77 since the last cyber security inspection	03.05
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	03.05

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 (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

(2) Vendor Manuals, Assessment and Corrective Actions:

a. The most recent Cyber-Security Quality Assurance (QA) audit and/or self-assessment

b. Corrective action documents (e.g., condition reports, including status of corrective actions) generate because 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 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.