



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

October 22, 2019

Mr. Ken J. 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 –  
NOTIFICATION OF CYBER SECURITY INSPECTION (NRC  
INSPECTION REPORT 05000445/2020401 AND  
05000446/2020401) AND REQUEST FOR INFORMATION

Dear Mr. Peters:

On February 10, 2020, the U.S. Nuclear Regulatory Commission (NRC) will begin an inspection in accordance with Inspection Procedure (IP) 71130.10P, "Cyber Security," Revision 0, at Comanche Peak Nuclear Power Plant, Units 1 and 2. This inspection evaluates and verifies your ability to meet the full implementation 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." The onsite portion of the inspection will take place during the weeks of February 10 and February 24, 2020.

Experience has shown that these inspections are extremely resource intensive, both for the NRC inspectors and the licensee staff. In order 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. The document request has been divided into four groups.

The first group specifies information necessary to assist the team in choosing the focus areas (i.e., "sample set") to be inspected in accordance with the cyber security inspection procedure. This information should be made available using either a secure document management service or passive media (i.e. CD, DVD) and delivered to the regional office no later than December 2, 2019. The inspection team will review this information and by the end of the planned information gathering visit on January 16, 2020, will request the specific items that should be provided for review.

The second group of requested documents will assist the team in their evaluation of the critical systems and critical digital assets, defensive architecture, and the areas of the cyber security plan selected for inspection. This information will be requested for our review in the regional office prior to the inspection, by January 27, 2020.

The third group of requested documents consists of those items that the team will review or need access to, during the inspection. Please have this information available by the first day of the onsite inspection, February 10, 2020.

The fourth group of information is necessary to aid the 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 Sam Graves. We understand that our regulatory contact for this inspection is Jim Barnette. If there are any questions about the inspection or the material requested, please contact the lead inspector at 817-200-1102 or by e-mail at [Samuel.Graves@nrc.gov](mailto:Samuel.Graves@nrc.gov).

This letter does not contain new or amended 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). 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, its enclosure, and your response (if any) 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 10 CFR 2.390, "Public Inspections, Exemptions, Requests for Withholding."

Sincerely,

/RA/

Nicholas H. Taylor, Chief  
Engineering Branch 2  
Division of Reactor Safety

Docket Nos. 05000445 and 05000446  
License Nos. NPF-87 and NPF-89

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

cc: Mr. Mike McNally  
Manager, Nuclear Security  
Comanche Peak Nuclear Power Plant  
Vistra Operations Company LLC  
6322 N FM 56  
P.O. Box 1002  
Glen Rose, TX 76043

COMANCHE PEAK NUCLEAR POWER PLANT, UNITS 1 AND 2 –  
 NOTIFICATION OF CYBER SECURITY INSPECTION (NRC INSPECTION  
 REPORT 05000445/2020401 AND 05000446/2020401) AND REQUEST FOR  
 INFORMATION – OCTOBER 22, 2019

**DISTRIBUTION:**

SMorris, ORA  
 MShaffer, ORA  
 TVegel, DRP  
 TInverso, DRP  
 RLantz, DRS  
 GMiller, DRS  
 MChambers, DRP  
 NDay, DRP  
 NO'Keefe, DRP  
 CAlldredge, DRP  
 JMelfi, DRP  
 NBrown, DRP  
 LReyna, DRP  
 VDricks, ORA  
 DGalvin, NRR  
 MHerrera, DRMA  
 R4Enforcement  
 DCylkowski, ORA  
 RAzua, DRS  
 PJayroe, DRS  
 JWeil, OWFN  
 AMoreno, OWFN  
 JQuichocho, OEDO  
 BMaier, ORA

ADAMS ACCESSION NUMBER: ML19295E162

☒ SUNSI Review: ADAMS: ☐ Non-Publicly Available ☒ Non-Sensitive Keyword:  
 By: STG ☒ Yes ☐ No ☒ Publicly Available ☐ Sensitive NRC-002

OFFICE	SRI:EB2	C:EB2				
NAME	SGraves	NTaylor				
SIGNATURE	/RA/	/RA/				
DATE	10/22/2019	10/22/2019				

OFFICIAL RECORD COPY

## Comanche Peak Nuclear Power Plant – Cyber Security Inspection Document Request

**Inspection Report:** 05000445/2020401 and 05000446/2020401

**Inspection Dates:** Weeks of February 10 and February 24, 2020

**Inspection Procedure:** IP 71130.10P, “Cyber Security,” Revision 0

**Reference 1:** ML17156A215 - “Guidance Document for Development of the Request for Information (RFI) and Notification Letter for Full-Implementation of the Cyber Security Inspection,” Revision 1, dated October 26, 2017

**NRC Inspectors:**

Sam Graves, Lead 817-200-1102 <a href="mailto:Samuel.Graves@nrc.gov">Samuel.Graves@nrc.gov</a>	Steven Alferink 817-200-1548 <a href="mailto:Steven.Alferink@nrc.gov">Steven.Alferink@nrc.gov</a>
David You, Observer 817-200-1233 <a href="mailto:David.You@nrc.gov">David.You@nrc.gov</a>	

**NRC Contractors:**

Alan Konkal 561-989-0210 <a href="mailto:Alan.Konkal@nrc.gov">Alan.Konkal@nrc.gov</a>	William Johns 301-287-3752 <a href="mailto:William.Johns@nrc.gov">William.Johns@nrc.gov</a>
---	---

### **I. Information Requested for In-Office Preparation**

The initial request for information (i.e., first RFI) provides the team with the general information necessary to select appropriate components and cyber security plan elements to develop a site-specific inspection plan. The team will use the first set of information requested to identify the list of critical systems and critical digital assets plus operational and management security control portions of the cyber security plan to be chosen as the “sample set” required to be inspected during this inspection. The first information request is specified in Table RFI #1. Provide the first set of information to the team lead in the regional office, by December 2, 2019, or sooner, to facilitate the selection of the specific items that will be reviewed during the onsite inspection weeks.

The required Table RFI #1 information shall be provided on a secure document management service or passive media (i.e. CD or DVD) to the lead inspector. Please provide five copies of each media submitted (i.e., one for each inspector/contractor). The preferred file format for all lists is a searchable Excel spreadsheet file on a CD or DVD. These files should be indexed and hyperlinked to facilitate efficient review. If you have any questions regarding this information, please contact the inspection team lead as soon as possible.

Enclosure

Table RFI #1		
<b>Section 3: Initial Documentation Requests (See Reference 1) Paragraph Number/Title:</b>		<b>Items</b>
1	List all identified critical systems and critical digital assets	All
2	List critical digital asset facility and site ethernet – transmission control protocol/internet protocol (TCP/IP) based local area networks (LANs) and identify those LAN's that have non-critical digital assets on them	All
3	List critical digital asset facility and site non-ethernet TCP/IP based LANs including those industrial networks and identify LANs that have non-critical digital assets on them	All
4	Network topology diagrams (be sure to include all network intrusion detection systems and security information and event management (SIEMs) for emergency preparedness (EP) networks and security level 3 and 4 networks)	All
8	List all network security boundary devices for EP networks and all network security boundary devices for levels 3 and 4	All
9	List critical digital asset wireless Industrial networks	All
11	Network Intrusion detection system documentation for critical systems that have critical digital assets associated with them	11.a.1) 11.a.2)
12	SIEM documentation for critical systems that have critical digital assets associated with them	12.a.1) 12.a.2)
14	List EP and security onsite and offsite digital communication systems	All
25	Cyber security assessment and cyber security incident response teams	All
28	Copy of current cyber security plan and copy of any 50.54(p) analysis to support changes to that plan	All
29	Copy of any licensee identified violations and associated corrective action program documentation to resolve issue(s)	All

In addition to the above information please provide the following:

- (1) Electronic copy of the updated safety analysis report and technical specifications
- (2) Name(s) and phone number(s) for the regulatory and technical contacts
- (3) Current management and engineering organizational charts related to cyber security
- (4) Cyber security program procedures

Based on this information, the team will identify and select specific systems and equipment (e.g., critical systems and critical digital assets) from the information requested by Table RFI #1 and submit a list of specific systems and equipment to your staff by the end of the information gathering visit on January 16, 2020, for the second information request (i.e., Table RFI #2).

## **II. Additional Information Requested to be Available Prior to Inspection**

As stated in Section I, the team will examine the documents from the initial information request and submit the list of specific systems and equipment to your staff by the end of the information gathering visit on January 16, 2020. This second information request (i.e., Table RFI #2) obtains additional documents required to evaluate the critical systems and critical digital assets, defensive architecture, and the areas of the cyber security program selected for the cyber security 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 Reference 1.

The Table RFI #2 information shall be provided on a secure document management service or passive media to the lead inspector, by January 27, 2020, or sooner. Please provide five copies of each CD/DVD submitted (i.e., one for each inspector/contractor). The preferred file format for all lists is a searchable Excel spreadsheet file on a CD/DVD. These files should be indexed and hyperlinked to facilitate efficient review. If you have any questions regarding this information, please call the inspection team lead as soon as possible.

Table RFI #2		
<b>Section 3: Initial Documentation Requests (See Reference 1) Paragraph Number/Title:</b>		<b>Items</b>
5	Plant computer system block diagram (if plant computer system is selected for inspection)	All
6	Plant security system block diagram (if security computer system is selected for inspection)	All
7	Block diagrams for distributed systems (for systems selected for inspection)	All
10	Host-based intrusion detection system documentation for critical digital assets (for systems selected for inspection)	10.a.1) 10.a.2)
13	List all maintenance and test equipment (M&TE) used on critical digital assets (for systems selected for inspection)	All
15	Configuration management	All
16	Supply chain management	16.a 16.b
17	Portable media and mobile device control	All
18	Software management	All
20	Vendor access and monitoring	All
21	Work control	All
22	Device access and key control	All
23	Password/authenticator policy	All

Table RFI #2	
Section 3: Initial Documentation Requests (See Reference 1) Paragraph Number/Title:	Items
24 User account/credential policy	All
26 Corrective actions since last NRC inspection	All
27 Cyber security assessments for selected systems	All

In addition to the above information please provide the following:

- (1) Names and positions of the CSAT and CSIRT members.
- (2) Copies of lessons plans and training presented to the CSAT and CSIRT members, continuing technical training for engineers, as well as any general awareness training.
- (3) List of dates of CSAT meetings that have occurred.

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

For the specific systems and equipment identified in Section II, provide the following request for information (i.e., Table 1st Week Onsite) on a secure document management service or passive media, by February 10, 2020, the first day of the inspection. All requested information shall follow the guidance in Reference 1.

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

Table 1 <sup>st</sup> Week Onsite	
Section 3: Initial Documentation Requests (See Reference 1) Paragraph Number/Title:	Items
10 Host-based intrusion detection system documentation for critical digital assets (for systems selected for inspection)	10.a.3) thru 10.a.12)
11 Network Intrusion detection system documentation for critical systems that have critical digital assets associated with them	11.a.3) thru 11.a.15)
12 SIEM documentation for critical systems that have critical digital assets associated with them	12.a.3) thru 12.a.14)
16 Supply chain management	16.c
19 Cyber security event notifications	All

Table 1 <sup>st</sup> Week Onsite	
Section 3: Initial Documentation Requests (See Reference 1) Paragraph Number/Title:	Items
29 Update to licensee identified violations and corrective action program actions taken since the initial request was made	All

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. Quality Assurance Plan;
  - b. Technical Specifications, if not previously provided;
  - c. Latest Individual Plant Examination/Probabilistic Risk Assessment Report; and,
- (2) Vendor Manuals, Assessments, and Corrective Actions:
  - a. The most recent cyber security quality assurance 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 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 team lead.