



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

March 5, 2019

Adam C. Heflin, President and
Chief Executive Officer
Wolf Creek Nuclear Operating Corporation
P.O. Box 411
Burlington, KS 66839

SUBJECT: WOLF CREEK GENERATING STATION – NOTIFICATION OF
CYBER SECURITY INSPECTION (NRC INSPECTION
REPORT 05000482/2019410) AND REQUEST FOR INFORMATION

Dear Mr. Heflin:

On July 15, 2019, the U.S. Nuclear Regulatory Commission (NRC) will begin an inspection in accordance with Inspection Procedure (IP) 71130.10P, "Cyber Security," Revision 0, at the Wolf Creek Generating Station (WC). 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 July 15 and July 29, 2019.

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 April 15, 2019. The inspection team will review this information and by the end of the planned information gathering visit on May 23, 2019, 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 June 17, 2019.

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, July 15, 2019.

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 Greg Pick. We understand that our regulatory contact for this inspection is Jason Knust. If there are any questions about the inspection or the material requested, please contact the lead inspector at 817-200-1270 or by e-mail at greg.pick@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 under 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.

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 10 CFR 2.390, "Public Inspections, Exemptions, Requests for Withholding."

Sincerely,

/RA Heather Gepford Acting For/

Francis C. Ramirez, Chief
Engineering Branch 1
Division of Reactor Safety

Docket: 50-482
License: NPF-42

Enclosure:
Wolf Creek Generating Station –
Cyber Security Inspection Document Request

cc w/ encl: Electronic Distribution

Wolf Creek Generating Station – Cyber Security Inspection Document Request

Inspection Report: 05000482/2019410

Inspection Dates: Weeks of July 15, 2019, and July 29, 2019

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:

Greg Pick, Lead 817-200-1270 greg.pick@nrc.gov	Steven Alferink 817-200-1548 steven.alferink@nrc.gov
---	---

NRC Contractors:

Casey Priester 703-725-9538 frederick.priester@nrc.gov	Cynthia DeBisschop 240-483-7938 cynthia.debisschop@nrc.gov
--	--

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 leader in the regional office by April 15, 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 by April 15, 2019. Please provide four 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 leader as soon as possible.

Enclosure

Table RFI #1		
Section 3: Initial Documentation Requests (See Reference 1) Paragraph Number/Title:		Items
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
- (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 May 23, 2019, 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 May 23, 2019. 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 June 17, 2019, or sooner. Please provide four 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 leader as soon as possible.

Table RFI #2	
Section 3: Initial Documentation Requests (See Reference 1) Paragraph Number/Title:	Items
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, 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 July 15, 2019, 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/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 ease of use. If you have any questions regarding this information, please call the inspection team leader as soon as possible.

Table 1 st 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
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 leader.

WOLF CREEK GENERATING STATION – NOTIFICATION OF CYBER SECURITY
INSPECTION (NRC INSPECTION REPORT 05000482/2019410) AND REQUEST FOR
INFORMATION – MARCH 5, 2019

DISTRIBUTION:

SMorris, ORA
MShaffer, ORA
TVegel, DRP
MHay, DRP
RLantz, DRS
GMiller, DRS
DDodson, DRP
FThomas, DRP
NTaylor, DRP
BTharakan, DRP
SGalemore, DRP
VDricks, ORA
BSingal, NRR
RKellar, DRS
PJayroe, DRS
MHerrera, DRMA
R4Enforcement
DCylkowski, ORA
JWeil, OWFN
AMoreno, OWFN
MMcCoppin, OEDO
BMaier, ORA

ADAMS ACCESSION NUMBER: ML19066A207

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

OFFICE	SRI:EB2	BC:EB2				
NAME	G. Pick	F. Ramirez				
SIGNATURE	/RA/	/RA HJG for/				
DATE	3/4/2019	3/5/2019				

OFFICIAL RECORD COPY