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

November 30, 2021

Mr. Fadi Diya, Senior Vice President
and Chief Nuclear Officer
Ameren Missouri Callaway Plant
8315 County Road 459
Steedman, MO 65077

SUBJECT: CALLAWAY PLANT - INFORMATION REQUEST FOR THE CYBER- SECURITY BASELINE INSPECTION, NOTIFICATION TO PERFORM INSPECTION 05000483/2022402

Dear Mr. Diya:

On March 28, 2022, the U.S. Nuclear Regulatory Commission (NRC) will begin a baseline inspection in accordance with Inspection Procedure (IP) 71130.10 “Cyber-Security,” Revision 0 at your Callaway Plant. 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 cyber-attacks in accordance with Title 10 of the Code of Federal Regulations (10 CFR) 73.54 and your approved cyber security 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. 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. 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 January 7, 2022. The inspection team will review this information and, by January 31, 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 February 28, 2022, as identified above.

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, March 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 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 Anthony Lowry of your organization. If there are any questions about the inspection or the material requested, please contact the lead inspector at 817-200-1102 or via e-mail at samuel.graves@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.

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 Graves, Samuel
on 11/30/21

Sam Graves, Senior Reactor Inspector
Engineering Branch 2
Division of Reactor Safety

Docket No.: 50-483
License No.: NPF-30
Enclosure: Cyber-Security Inspection Document Request
cc w/encl: Distribution via LISTSERV®

CALLAWAY PLANT - INFORMATION REQUEST FOR THE CYBER-SECURITY BASELINE INSPECTION, NOTIFICATION TO PERFORM INSPECTION 05000483/2022402 – DATED NOVEMBER 30, 2021.

DISTRIBUTION:
SMorris, RA
Jmonninger, DRA
TVegel, DRP
MHay, DRP
RLantz, DRS
JDixon, DRS
RWilliams, RIV/OEDO (Robert)
VDricks, ORA
LWilkins, OCA
MChawla, NRR
AMoreno, RIV/OCA
BMaier, RSLO
FRamirez, IPAT
GWerner, DRP
DProulx, DRP
JMelfi, DRP
HStrittmatter, DRP
ASmallwood, DRP
DBradley, DRP
SJanicki, DRP
DYancey, DRP
LFlores, IPAT
R4Enforcement

ADAMS ACCESSION NUMBER: ML21333A157

X SUNSI Review By: STG	ADAMS: ■ Yes ☐ No	☐ Sensitive ■ Non-Sensitive	☐ Non-Publicly Available ■ Publicly Available	Keyword NRC-002
OFFICE	EB2:SRI			
NAME	S. Graves			
SIGNATURE	***/RA/***			
DATE	11/30/2021			

OFFICIAL RECORD COPY

Inspection Report: 05000483/2022401

Inspection Dates: Onsite the week of March 28, 2022

Inspection Procedure: IP 71130.10, "Cyber-Security," Revision 0

Reference: "Guidance Document for Development of the Request for Information (RFI) and Notification Letter for Full-Implementation of the Cyber-Security Inspection." (ML TBD)

NRC Inspectors:
Sam Graves, Lead
817-200-1102
samuel.graves@nrc.gov

Stella Opara
301-287-9286
stella.opara@nrc.gov

NRC Contractors:
Alan Konkal
561-989-0210
alan.konkal@nrc.gov

Casey Priester
301-415-7000
frederick.priester@nrc.gov

I. Information Requested for In-Office Preparation

This initial request for information (i.e., first RFI) 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 Table RFI #1 to the regional office by January 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 January 31, 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 February 28, 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.

The required Table RFI 1 information shall be provided on digital media (CD/DVD)) or an online document repository to the lead inspector by January 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 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, and non-CDA digital assets used in the cyber defensive architecture, (e.g., firewalls, SIEM, NIDS/NIPS, kiosks, access authorization, 10 CFR 73.55 equipment not part of the security system) – highlight/note any changes (e.g., additions, deletions, reclassifications) since the last cyber security inspection, including changes to boundary devices	Overall
2	A list of CDA and DA wireless Industrial networks	Overall
3	A list of EP and Security onsite and offsite digital communication systems	Overall
4	Network Topology Diagrams	Overall
5	Ongoing Monitoring and Assessment program documentation	03.01(a)
6	The most recent effectiveness analysis of the Cyber Security Program	03.01(b)
7	Vulnerability screening/assessment and scan program documentation	03.01(c)
8	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)
9	List of all network security boundary devices for EP networks and all network security boundary devices for levels 3 and 4	03.02(b)
10	Device Access and Key Control documentation	03.02(c)
11	Password/Authenticator documentation	03.02(c)
12	User Account/Credential documentation	03.02(d)

Table RFI #1		
Section 3, Paragraph Number/Title:		**IP Ref**
13	Portable Media and Mobile Device control documentation, including kiosk security control assessment/documentation	03.02(e)
14	List of all design changes completed since the last inspection, including 50.59 documentation and the design changes/modifications program documentation	03.03(a)
15	Supply Chain Management documentation including any security impact analysis for new acquisitions	03.03(a), (b) and (c)
16	Configuration Management documentation including any security impact analysis performed due to configuration changes since the last inspection	03.03(a) and (b)
17	Cyber Security Plan and any 50.54(p) analysis to support changes to the plan since the last inspection	03.04(a)
18	Cyber Security Assessment team documentation to include any training documentation (both general cyber security training and any specialized training	03.04(c)
19	Cyber Security Metrics tracked (if applicable)	03.05(b)
21	Provide a list of all procedures and policies provided to the NRC with their descriptive name and associated number	Overall

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 January 31, 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 January 31, 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 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 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 February 28, 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 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	Any effectiveness analysis for the security controls that have been performed on the system(s)	03.01(b)
4	All vulnerability screenings/assessments associated with or scans performed on the selected system(s) since the last inspection	03.01(c)
5	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)
6	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)
7	Copies of all periodic reviews of the access authorization list for the selected systems since the last inspection	03.02(d)

Table RFI #2		
Section 3, Paragraph Number/Title:		**Items**
8	Baseline configuration data sheets for the selected system(s)	03.03(a)
9	Documentation on any changes, including Security Impact Analyses, performed on the selected system(s) since the last inspection	03.03(b)
10	Copies of the purchase order documentation for any new equipment purchased for the selected systems since the last inspection	03.03(c)
11	Copies of any cyber security drills performed since the last inspection	03.02(a) 03.04(b)
12	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)
13	Corrective actions taken because of cyber security incidents/issues to include previous NRC violations and Licensee Identified Violations since the last cyber security inspection	03.04(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 1ST Week Onsite) on digital media (CD/DVD) or an online document repository by March 28, 2022, the first day of the inspection. All requested information shall follow the guidance document referenced above.

Please provide four copies of each 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 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 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, 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) 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.