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

July 15, 2025

Khalil Dia, Site Vice President
Nebraska Public Power District
72676 648A Avenue
P.O. Box 98
Brownville, NE 68321

SUBJECT: COOPER NUCLEAR STATION - INFORMATION REQUEST FOR THE "CYBER- SECURITY" BASELINE INSPECTION, NOTIFICATION TO PERFORM INSPECTION 05000298/2025401

Dear Khalil Dia:

On September 15, 2025, the U.S. Nuclear Regulatory Commission (NRC) will begin a baseline inspection in accordance with Inspection Procedure (IP) 71130.10 "Cyber-Security," at your Cooper Nuclear Station. The inspection will be performed to evaluate and verify 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 either in an online repository (preferred) or digital media (CD/DVD) and delivered/available to the regional office no later than August 1, 2025. The inspection team will review this information and, by August 15, 2025, 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, 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 September 2, 2025.

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, September 15, 2025.

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 all 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 Shiattin Makor. We understand that our regulatory contact for this inspection is Brian Sander of your organization. If there are any questions about the inspection or the material requested, please contact the lead inspector at (817) 200-1507 or via e-mail at shiattin.makor@nrc.gov.

Paperwork Reduction Act Statement

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, 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.

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 Makor, Shiattin
on 07/15/25

Shiattin Makor, Senior Reactor Inspector
Engineering Branch 2
Division of Operations and Reactor Safety

Docket No. 05000298
License No. DPR-46

Enclosure: Cooper Nuclear Station
Cyber-Security Inspection
Request for Information

cc w/encl: Distribution via LISTSERV

COOPER NUCLEAR STATION – INFORMATION REQUEST FOR THE "CYBER-SECURITY" BASELINE INSPECTION, NOTIFICATION TO PERFORM INSPECTION 05000298/2025401 – DATED JULY 15, 2025

DISTRIBUTION:
JMonninger, ORA
GMiller, DORS
NTaylor, DORS
DCylkowski, RC
TSteadham, RIV/OEDO
VDricks, ORA
TSmith, ORA
LWilkins, OCA
JDrake, NRR
AMoreno, RIV/OCA
RAlexander, RSLO
DDodson, DORS
ABetts, DORS
DOuk, DORS
CWynar, DORS
EPowell, DORS
LDay, DORS
R4DORS-IPAT
R4Enforcement
SOSB Insp Rpt Distro
SOSBInspRptDistro@usnrc.onmicrosoft.com

DOCUMENT NAME: COOPER NUCLEAR STATION – INFORMATION REQUEST FOR THE "CYBER-SECURITY" BASELINE INSPECTION, NOTIFICATION TO PERFORM INSPECTION 05000298/2025401
ADAMS ACCESSION NUMBER: **ML25196A463**

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

OFFICE	BC:DORS/EB2	SRI:DORS/EB2		
NAME	GWarnick	SMakor		
SIGNATURE	***/RA/***	***/RA/***		
DATE	07/15/25	07/15/25		

OFFICIAL RECORD COPY

Cooper Cyber-Security Inspection Request for Information

Inspection Report:	05000298/2025401	
Inspection Dates:	September 15 to 19, 2025	
Inspection Procedure:	IP 71130.10, "Cyber-Security,"	
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:	Shiattin Makor, Lead (817) 200-1507 shiattin.makor@nrc.gov	Andrew Saunders (817) 200-1275 andrews.saunders@nrc.gov
NRC Contractors:	Balla Barro ballo.barro@nrc.gov	Charles Simpson charles.simpson@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 inspection procedure. Please provide the information requested in Table RFI #1 to the regional office by August 1, 2025, 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 August 15, 2025, 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 September 2, 2025. All requests for information shall follow the referenced guidance document. For information requests that have more than ten (10) documents, provide a compressed (i.e., Zip) file of the documents.

The required Table RFI #1 information shall be provided in an online document repository (preferred) or on digital media (CD/DVD) to the lead inspector by August 1, 2025. 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. 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	Network Topology Diagrams to include information and data flow for critical systems in levels 2, 3 and 4 (If available)	Overall
3	The most recent effectiveness analysis and self-assessments of the Cyber-Security Program	03.01(b)
4	Portable Media and Mobile Device control documentation, including kiosk security control assessment/documentation	03.02(e)
5	Design change/modification program documentation and a list of all cyber-related design changes completed since the last two Cyber-Security inspections, including either a summary describing the design change or the 50.59 documentation for the change.	03.03(a)
6	Cyber-Security Plan and any 50.54(p) analysis to support changes to the plan since the last inspection	03.04(a)
7	Provide copies of all Cyber-Security program related procedures, program documentation, and policies with their **descriptive name** and associated number (if available), including supply chain, vulnerability management, ongoing monitoring and assessment	Overall 03.01(a) 03.03(a), (b), and (c)
8	Corrective actions taken because of Cyber-Security incidents/issues to include previous NRC violations and Licensee Identified Violations since two last Cyber-Security inspections	03.05

In addition to the above information please provide the following:

(1) Electronic copy of the operating license.

(2) Name(s) and phone numbers for the regulatory and technical contacts.

(3) Current management and engineering organizational charts.

Based on this information, the inspection team will identify and select specific systems and equipment (e.g., critical systems/critical digital assets) from the information requested by Table RFI #1 and submit a list of specific systems and equipment to your staff by August 1, 2025, 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 August 1, 2025, for the second RFI (i.e., RFI #2). The second RFI will request additional information required to evaluate the critical systems and critical digital assets, defensive architecture, and the areas of the Cyber-Security program selected for inspection. The additional information requested for the specific systems and equipment is identified in Table RFI #2. All requested information shall follow the referenced guidance document.

The Table RFI #2 information shall be provided in an online document repository (preferred) or on digital media (CD/DVD) to the lead inspector by September 2, 2025. The preferred file format for all lists is a searchable Excel spreadsheet. 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 #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) and critical digital assets	03.01(a)
2	All Security Control Assessments for the selected critical system(s) and critical digital assets.	03.01(a)
3	All vulnerability screenings/assessments associated with, or scans performed on the selected system(s) and critical digital assets 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	03.02(b)

Table RFI #2		
Section 3, Paragraph Number/Title:		**Items**
	Intrusion Detection Systems (HIDS), and Security Information and Event Management (SIEM) systems for system(s) chosen for inspection	
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	Baseline configuration information for the selected critical digital assets	03.03(a)
7	Documentation on any changes, including Security Impact Analyses, performed on the selected system(s) since the last inspection, including security impact analyses for replacement critical digital assets	03.03(b)
8	Copies of the purchase order documentation for any new equipment purchased for the selected systems since the last inspection.	03.03(c)
9	Copies of any reports/assessment for Cyber-Security drills performed since the last inspection.	03.02(a) 03.04(b)
10	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)
11	Cyber-Security Incident response documentation, including incident detection, response, and recovery documentation as well as contingency plan development, implementation including any program documentation that requires testing of security boundary device functionality	03.02(a) and 03.04(b)
12	Device Access and Key Control documentation	03.02(c)
13	User Account/Credential documentation	03.02(d)
14	Password/Authenticator documentation	03.02(c)
15	Configuration Management documentation including any security impact analysis performed due to configuration changes since the last inspection	03.03(a) and (b)
16	Provide documentation describing any Cyber-Security changes to the access authorization program since the last Cyber-Security inspection.	Overall

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) to the team by September 15, 2025, the first day of the inspection. All requested information shall follow the referenced guidance document.

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 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 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	03.04(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 if the inspectors have easy and unrestrained access to them.

   a. Original SER and Supplements related to Cyber-Security;

   b. FSAR Question and Answers related to Cyber-Security; and

   c. Quality Assurance Plan.

(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) generated 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.