



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

June 26, 2023

John Dent, Jr.  
Executive Vice President and Chief Nuclear Officer  
Nebraska Public Power District  
Cooper Nuclear Station  
72676 648A Avenue  
P.O. Box 98  
Brownville, NE 68321

SUBJECT: COOPER NUCLEAR STATION – INFORMATION REQUEST FOR THE  
CYBERSECURITY BASELINE INSPECTION, NOTIFICATION TO PERFORM  
INSPECTION 05000298/2023401

Dear John Dent, Jr.

On September 18, 2023, the U.S. Nuclear Regulatory Commission (NRC) will begin a baseline inspection in accordance with Inspection Procedure (IP) 71130.10, "Cybersecurity," at your Cooper Nuclear Station. 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 cyberattacks in accordance with Title 10 of the Code of Federal Regulations (10 CFR) 73.54 and your approved cybersecurity 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 cyber security inspections are extremely resource intensive, both for the NRC inspectors and 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 cybersecurity 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 July 21, 2023. The inspection team will review this information and, by August 4, 2023, 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 September 8, 2023, 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, September 18, 2023.

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 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 Philipp Braaten. We understand that our regulatory contact for this inspection is Mark Unruh of your organization. If there are any questions about the inspection or the material requested, please contact the lead inspector at 404-997-4651 or via e-mail at Philipp.braaten@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 under approval number 3150-0011. The burden to the public for these information collections is estimated to average 40 hour(s) per response. Send comments regarding this information collection to the FOIA, Library and Information Collection Branch, Office of the Chief Information Officer, Mail Stop: T6-A10M, U.S. Nuclear Regulatory Commission, Washington, DC 20555-0001, or by email to [Infocollects.Resource@nrc.gov](mailto:Infocollects.Resource@nrc.gov), and to the Desk Officer, Office of Information and Regulatory Affairs, NEOB-10202, (3150-0011) OMB, Washington, DC 20503.

### **Public Protection Notification**

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).

J. Dent, Jr.

3

Sincerely,



Signed by Sacko, Fanta  
on 06/26/23

Fanta Sacko, Branch Chief  
Engineering Branch 2  
Division of Operating Reactor Safety

Docket No. 50-298  
License No. DPR-46

Enclosure: Cooper Nuclear Station Cyber-Security Inspection Document Request

cc w/encl: Distribution via LISTSERV

COOPER NUCLEAR STATION – INFORMATION REQUEST FOR THE CYBERSECURITY BASELINE INSPECTION, NOTIFICATION TO PERFORM INSPECTION 05000298/2023401 – DATED JUNE 26, 2023.

**DISTRIBUTION:**

PBraaten, RII  
NOkonkwo, RIV  
JJosey, RIV  
KChambliss, RIV

COOPER NUCLEAR STATION – INFORMATION REQUEST FOR THE CYBERSECURITY BASELINE INSPECTION, NOTIFICATION TO PERFORM INSPECTION 05000298/2023401

ADAMS ACCESSION NUMBER: **ML23173A086**

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

OFFICE	RII: DRS/EB2	RIV:DORS/EB2		
NAME	PBraaten	FSacko		
SIGNATURE	/RA/	/RA/		
DATE	06/22/23	06/26/23		

**OFFICIAL RECORD COPY**

# WATERFORD STEAM ELECTRIC STATION CYBER-SECURITY INSPECTION DOCUMENT REQUEST

**Inspection Report:** 05000298/2023401

**Inspection Dates:** Week of September 18, 2023

**Inspection Procedure:** IP 71130.10, "CYBERSECURITY"

**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:**

Philipp Braaten, Lead 404-997-4651 <a href="mailto:philipp.braaten@nrc.gov">philipp.braaten@nrc.gov</a>	Nnaerika Okonkwo 817-200-1114 <a href="mailto:nnaerika.okonkwo@nrc.gov">nnaerika.okonkwo@nrc.gov</a>
---	--

**NRC Contractors:**

Michael Shock 301-415-7000 <a href="mailto:michael.shock@nrc.gov">michael.shock@nrc.gov</a>	Trace Coleman 301-415-7000 <a href="mailto:trace.coleman@nrc.gov">trace.coleman@nrc.gov</a>
---	---

## ***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 list of critical systems and critical digital assets (CSs/CDAs) plus operational and management (O&M) security control portions of the CSP to be chosen as the "sample set" required to be inspected by the cybersecurity IP. The first RFI's requested information is specified below in Table RFI #1. Please provide the information requested in Table RFI #1 to the regional office by **July 21, 2023**, 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 4, 2023**, which will be utilized to evaluate the equipment, defensive architecture, and the areas of the cyber security program for review during the inspection.

Please provide the information requested by the second RFI to the regional office by **September 8, 2023**. 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.

Enclosure

The required Table RFI #1 information shall be provided on digital media (CD/DVD)) or an online document repository to the lead inspector by **July 21, 2023**. 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 contact the inspection team leader as soon as possible.

<b>Table RFI #1</b>	
<b>Paragraph Number/Title:</b>	<b>IP Ref</b>
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 program 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 program documentation.	03.02(c)
9 Password/Authenticator program documentation.	03.02(c)
10 User Account/Credential and Authentication program documentation.	03.02(d)
11 Portable Media and Mobile Device control program 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, including either a summary of the design change or the 50.59 documentation for the change.	03.03(a)
13 Supply Chain Management program documentation including a list of security impact analysis for new acquisitions.	03.03(a), (b) and (c)

**WATERFORD STEAM ELECTRIC STATION CYBER-SECURITY INSPECTION DOCUMENT  
REQUEST**

<b>Table RFI #1</b>	
<b>Paragraph Number/Title:</b>	<b>IP Ref</b>
14 Configuration Management program documentation including a list of security impact analysis performed due to configuration changes since the last cyber 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 Performance 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 cyber security procedures and policies with their descriptive name and associated number.	Overall
19 Performance testing report (if applicable).	03.06(a)
20 Electronic Copy of UFSAR and Technical Specifications	Overall

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 **August 4, 2023**, 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 4, 2023**, 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 cybersecurity 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 **September 8, 2023**. The preferred file format for all lists is a searchable Excel spreadsheet file. The submitted information should be indexed and hyper-linked to facilitate ease of use. If you have any questions regarding this information, please contact the inspection team leader as soon as possible.

<b>Table RFI #2</b>	
<b>Paragraph Number/Title:</b>	<b>Items</b>
<b>For the system(s) chosen for inspection provide:</b>	
1 Ongoing Monitoring and Assessment activity performed on the selected 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 cyber 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 List 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.	03.05

*\*Some selected systems may have a large number of CDAs. For these systems reach out to the team leader for a specific selection of CDAs when responding to this request.*

## WATERFORD STEAM ELECTRIC STATION CYBER-SECURITY INSPECTION DOCUMENT REQUEST

### **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 Onsite Week) on digital media (CD/DVD) or an online document repository by September 18, 2023, the first day of the inspection. All requested information shall follow the guidance document referenced above.

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 contact the inspection team leader as soon as possible.

Table Onsite Week		
	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	03.05

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. Current FSAR Volume;
  - c. SER and Supplements for Cybersecurity Program;
  - d. FSAR Question and Answers related to Cybersecurity Program;
  - e. Quality Assurance Plan for Cybersecurity;
  - f. Technical Specifications, if not previously provided;
- (2) Vendor Manuals for the CDAs selected
- (3) Assessments 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 as a result 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 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 inspection team leader.