UNITED STATES
NUCLEAR REGULATORY COMMISSION
REGION III
2443 WARRENVILLE ROAD, SUITE 210
LISLE, ILLINOIS 60532-4352

January 12, 2021

Mr. Joel P. Gebbie
Senior VP and Chief Nuclear Officer
Indiana Michigan Power Company
Nuclear Generation Group
One Cook Place
Bridgman, MI 49106

SUBJECT: DONALD C. COOK NUCLEAR POWER PLANT, UNITS 1 AND 2 — INFORMATION REQUEST FOR THE CYBER-SECURITY FULL IMPLEMENTATION INSPECTION, NOTIFICATION TO PERFORM INSPECTION 05000315/2021401; 05000316/2021401

Dear Mr. Gebbie:

On November 19, 2019, the U.S. Nuclear Regulatory Commission (NRC) provided the Donald C. Cook Nuclear Power Plant, Units 1 and 2, an Information Request for the Cyber-Security Full Implementation Inspection and Notification to Perform Inspection 05000315/2020410; 05000316/2020410 (ML19323F427). The onsite portion of this inspection was to take place during the weeks of March 30, 2020, and April 13, 2020. However, because of the coronavirus pandemic (COVID-19) and potential related health concerns, the inspection was delayed by the NRC.

Based on discussions with your staff for an acceptable date to perform this inspection, the NRC has rescheduled this inspection. The onsite portion of the inspection will take place during the weeks of June 7 and June 21, 2021. The inspection will be performed in accordance with Inspection Procedure 71130.10P "Cyber-Security," issued May 15, 2017, at your Donald C. Cook Nuclear Power Plant, Units 1 and 2. The inspection will be performed to evaluate and verify your ability to meet full implementation requirements of the NRC's Cyber-Security Rule, Title 10 of the *Code of Federal Regulations*, Part 73, Section 54, "Protection of Digital Computer and Communication Systems and Networks."

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, the November 19, 2019, letter (ML19323F427) enclosed a request for documents needed for the inspection. These documents were divided into four groups.

- The first group specified 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 and the specific items to be reviewed have been previously provided to the regional office.

- The second group of additional 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 plant's Cyber-Security Program selected for the Cyber-Security

Inspection. This information and the specific items to be reviewed have been previously provided to the regional office.

- 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, June 7, 2021.

- The fourth group of information is necessary to aid the inspection 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 George M. Hausman. We understand that our regulatory contact for this inspection is Kristen M. Harper of your organization. If there are any questions about the inspection or the material requested, please contact the lead inspector at 630-829-9743 or via e-mail at George.Hausman@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, 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 Title 10 of the *Code of Federal Regulations*, Part 2.390, "Public Inspections, Exemptions, Requests for Withholding."

Sincerely,

/RA/

George M. Hausman, Senior Reactor Inspector
Engineering Branch 3
Division of Reactor Safety

Docket Nos. 50–315; 50–316
License Nos. DPR–58; DPR–74

Enclosure:
Document Request for Cyber-Security Inspection

cc: Distribution via LISTSERV®

Letter to Joel P. Gebbie from George M. Hausman dated January 12, 2021.

SUBJECT: DONALD C. COOK NUCLEAR POWER PLANT, UNITS 1 AND 2 — INFORMATION REQUEST FOR THE CYBER-SECURITY FULL IMPLEMENTATION INSPECTION, NOTIFICATION TO PERFORM INSPECTION 05000315/2021401; 05000316/2021401

DISTRIBUTION:
Jessie Quichocho
Richard Skokowski
RidsNrrDorlLpl3
RidsNrrPMDCCook Resource
RidsNrrDroIrib Resource
John Giessner
Kenneth O'Brien
Jamnes Cameron
Allan Barker
DRPIII
DRSIII

ADAMS Accession Number: ML21012A059
☒ Publicly Available ☐ Non-Publicly Available ☐ Sensitive ☒ Non-Sensitive

OFFICE	RIII						
NAME	GHausman:mb via e-mail						
DATE	01/12/2021						

OFFICIAL RECORD COPY

DOCUMENT REQUEST FOR CYBER-SECURITY INSPECTION

Inspection Report:	05000315/2021401; 05000316/2021401
Inspection Dates:	Weeks of June 7, 2021, and June 21, 2021
Inspection Procedure:	71130.10P, "Cyber-Security," Issue Date May 15, 2017
Reference:	Guidance Document for Development of the Request for Information and Notification Letter for Full-Implementation of the Cyber-Security Inspection, Issue Date October 26, 2017 (ML17156A215)

NRC Inspectors:	George M. Hausman, Lead 630-829-9743 George.Hausman@nrc.gov	Jasmine A. Gilliam 630-829-9831 Jasmine.Gilliam@nrc.gov
NRC Contractors:	Alan B. Konkal 561-989-0210 Alan.Konkal@nrc.gov	Alexander R. Prada 240-449-5791 Alexander.Prada@nrc.gov
Observer:	TBD NSIR/DPCP/CSB	

I Information Requested for In-Office Preparation

The initial request for information (i.e., first Request for Information (RFI)) concentrates on providing the inspection team with the general 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 (CSs) and critical digital assets (CDAs) plus operational and management security control portions of the Cyber-Security Program to be chosen as the "sample set" required to be inspected by the Cyber-Security Inspection Procedure. The first RFI's requested information is specified below in Table RFI #1. The Table RFI #1 information has been previously provided to the regional office to facilitate the selection of the specific items that will be reviewed during the onsite inspection weeks.

The inspection team has examined the returned documentation from the first RFI and identified/selected specific systems and equipment (e.g., CSs/CDAs) to provide a more focused follow-up request to develop the second RFI. The inspection team has previously provided the specific systems and equipment list to your staff which identified the specific systems and equipment that will be utilized to evaluate the CSs/CDAs, defensive architecture, and the areas of the licensee's CSP selected for the Cyber-Security Inspection. All requests for this information shall follow the Table RFI #1 and the guidance document referenced above.

The required Table RFI #1 information has been previously provided.

Table RFI #1

Reference Section 3, Paragraph Number/Title:		Items
1	List All Identified CSs and CDAs	All
2	List CDA Facility and Site Ethernet—Transmission Control Protocol/Internet Protocol Based Local Area Networks (LANs) and Identify Those LANs That Have Non-CDAs on Them	All
3	List CDA Facility and Site Non-Ethernet Transmission Control Protocol/Internet Protocol Based LANs Including Those Industrial Networks and Identify LANs That Have Non-CDAs on Them	All
4	Network Topology Diagrams (Be Sure to Include All Network Intrusion Detection System and Security Information and Event Managements (SIEM) 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 CDA Wireless Industrial Networks	All
11	Network Intrusion Detection System Documentation for CSs That Have CDAs Associated with Them	11.a.1) 11.a.2)
12	SIEM Documentation for CSs That Have CDAs 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 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 ensure the following information has been provided to the inspection team:

(1) Electronic copy of the Updated Finals Safety Analysis Report and technical specifications.

(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 has previously identified and selected the specific systems and equipment (e.g., CSs/CDAs) from the information requested by Table RFI #1 and has previously submitted a list of specific systems and equipment to your staff for the second RFI (i.e., Table RFI #2).

II Additional Information Requested to Be Available Prior to Inspection

As stated above, in Section I of this enclosure, the inspection team examined the returned documentation requested from Table RFI #1 and has previously submitted the list of specific systems and equipment to your staff for the second RFI (i.e., RFI #2). The second RFI requested 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 requests for this information shall follow the Table RFI #2 and the guidance document referenced above.

The Table RFI #2 information has previously been submitted on CD to the lead inspector. If you have any questions regarding this information, please call the inspection team leader as soon as possible.

Table RFI #2

Reference Section 3, 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	Systems That Are Distributed Block Diagrams (For Systems Selected for Inspection)	All
10	Host-Based Intrusion Detection System Documentation (For CDAs for Systems Selected for Inspection)	10.a.1) 10.a.2)
13	List All Maintenance and Test Equipment Used on CDAs for Systems Selected for Inspection	All
15	Configuration Management	All
16	Supply Chain Management	16.b. 16.c.1) 16.c.5) 16.c.6)
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
24	User Account/Credential Policy	All
26	Corrective Actions Since Last U.S. Nuclear Regulatory Commission Inspection	All
27	Cyber Security Assessments for Selected Systems	All

III Information Requested to Be Available on First Day of Inspection

For the specific systems and equipment identified in this enclosure's Section II, provide the following RFI (i.e., Table 1st Week Onsite) on CD by June 7, 2021, the first day of the inspection. All requests for this information shall follow the Table 1st Week Onsite and the guidance document referenced above.

Please provide five 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. These CDs 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

Reference Section 3, Paragraph Number/Title:		Items
10	Host-Based Intrusion Detection System Documentation for CDAs for Systems Selected for Inspection	10.a.3) thru 10.a.12)
11	Network Intrusion Detection System Documentation for CSs That Have CDAs Associated with Them	11.a.3) thru 11.a.15)
12	SIEM Documentation for CSs That Have CDAs Associated with Them	12.a.3) thru 12.a.14)
16	Supply Chain Management	16.c.2) 16.c.3) 16.c.4)
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. Original Final Safety Analysis Report Volumes;
b. Original Safety Evaluation Report and Supplements;
c. Final Safety Analysis Report Question and Answers;
d. Quality Assurance Plan;
e. Latest Individual Plant Examination/Probabilistic Risk Assessment Report; and
f. Vendor Manuals.

(2) Assessment 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 inspection team leader.