UNITED STATES
NUCLEAR REGULATORY COMMISSION
REGION III
2443 WARRENVILLE RD. SUITE 210
LISLE, IL 60532-4352

June 8, 2017

Mr. Peter A. Gardner
Site Vice President
Monticello Nuclear Generating Plant
Northern States Power Company, Minnesota
2807 West County Road 75
Monticello, MN 55362–9637

SUBJECT: MONTICELLO NUCLEAR GENERATING PLANT, UNIT 1 – INFORMATION REQUEST FOR THE "CYBER-SECURITY" BASELINE INSPECTION, NOTIFICATION TO PERFORM INSPECTION 05000263/2017409

Dear Mr. Gardner:

On September 11, 2017, the U.S. Nuclear Regulatory Commission (NRC) will begin a baseline inspection in accordance with Inspection Procedure 71130.10P "Cyber-Security," issued May 15, 2017, at your Monticello Nuclear Generating Plant, Unit 1. 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, *Code of Federal Regulations*, 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 September 11–15, 2017, and September 25–29, 2017.

Experience has shown that baseline 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. 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 via compact disc and delivered to the regional office no later than July 7, 2017. The inspection team will review this information and, by July 24, 2017, will request the specific items that should be provided for review.

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 will be requested for review in the regional office prior to the inspection by August 11, 2017.

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 11, 2017.

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 Mr. George M. Hausman. We understand that our regulatory contact for this inspection is Mr. Steven Sollom 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 10 CFR 2.390, “Public Inspections, Exemptions, Requests for Withholding.”

Sincerely,

/RA/

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

Docket No. 50–263
License No. DPR–22

Enclosure:
Cyber-Security Inspection Document Request

cc: Distribution via LISTSERV®

Letter to Peter A. Gardner from George Hausman dated June 8, 2017

SUBJECT: MONTICELLO NUCLEAR GENERATING PLANT, UNIT 1 – INFORMATION REQUEST FOR THE "CYBER-SECURITY" BASELINE INSPECTION, NOTIFICATION TO PERFORM INSPECTION 05000263/2017409

DISTRIBUTION:
Jeremy Bowen
RidsNrrDorlLpl3
RidsNrrPMMonticello
RidsNrrDirsIrib Resource
Cynthia Pederson
Darrell Roberts
Richard Skokowski
Allan Barker
Carole Ariano
Linda Linn
DRPIII
DRSIII

ADAMS Accession Number ML17159A699

OFFICE	RIII		RIII		RIII		RIII	
NAME	GHausman:cl							
DATE	06/08/17							

OFFICIAL RECORD COPY

CYBER-SECURITY INSPECTION DOCUMENT REQUEST

Inspection Report: 05000263/2017409

Inspection Dates: September 11–15, 2017
September 25–29, 2017

Inspection Procedure: IP 71130.10P, "Cyber-Security," Issue Date: May 15, 2017

Reference: Guidance Document for Development of the Request for Information (RFI) and Notification Letter for Full-Implementation of the Cyber-Security Inspection, Issue Date May 25, 2017

NRC Inspectors:

George M. Hausman, Lead
630-829-9743
George.Hausman@nrc.gov

Dariusz Szwarc
630-829-9803
Dariusz.Szwarc@nrc.gov

NRC Contractors:

F. Casey Priester
703-725-9538
Frederick.Priester@nrc.gov

John A. Walley
703-999-9098
John.Walley@nrc.gov

Observers:

Gregory A. Pick
817-200-1270
Greg.Pick@nrc.gov

Samuel T. Graves
817-200-1102
Samuel.Graves@nrc.gov

James D. Beardsley
301-287-0908
James.Beardsley@nrc.gov

Robert C. Daley
630-829-9749
Robert.Daley@nrc.gov

Ralph H. Costello
301-287-3618
Ralph.Costello@nrc.gov

Catherine J. Allen
301-287-3620
Catherine.Allen@nrc.gov

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 (CSP) 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 security control portions of the CSP 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 is requested to be provided to the regional office by July 7, 2017, or sooner, to facilitate the selection of the specific items that will be reviewed during the onsite inspection weeks.

The inspection team will examine the returned documentation from the first RFI and identify/select specific systems and equipment (e.g., CSs/CDAs) 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 July 24, 2017, which will identify 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 shall be provided on compact disc (CD) to the lead inspector by July 7, 2017. Please provide five copies of each CD submitted (i.e., one for each inspector/contractor and one for the observers). 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 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 LAN's That Have Non-CDA's 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-CDA's On Them	All
4	Network Topology Diagrams (Be Sure To Include All Network Intrusion Detection System (NIDS) 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 CDA Wireless Industrial Networks	All
11	NIDS Documentation for Critical Systems That Have CDAs Associated with Them	11.a.1) 11.a.2)
12	SIEM Documentation for Critical Systems 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

In addition to the above information please provide the following:

(1) Electronic copy of the Updated Final 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 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 July 24, 2017, 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 will examine the returned documentation requested from Table RFI #1 and submit the list of specific systems and equipment to your staff by July 24, 2017, for the second RFI (i.e., Table 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 requests for this information shall follow the Table RFI #2 and the guidance document referenced above.

The Table RFI #2 information shall be provided on CD to the lead inspector by August 11, 2017. Please provide five copies of each CD submitted (i.e., one for each inspector/contractor and one for the observers). 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 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.a. 16.b.1) 16.b.5) 16.b.6)
17	Portable Media and Mobile Device Control	All
18	Software Management	All
20	Vendor Access and Monitoring	All
21	Work Control	All

Table RFI #2		
Reference Section 3, Paragraph Number/Title:		**Items**
22	Device Access and Key Control	All
23	Password/Authenticator Policy	All
24	User Account/Credential Policy	All
26	Corrective Actions Since Last NRC Inspection	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 compact disc (CD) by September 11, 2017, 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 and one for the observers). 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	NIDS Documentation for Critical Systems That Have CDAs Associated with Them	11.a.3) thru 11.a.15)
12	SIEM Documentation for Critical Systems That Have CDAs Associated with Them	12.a.3) thru 12.a.14)
16	Supply Chain Management	16.b.2) 16.b.3) 16.b.4)
19	Cyber-Security Event Notifications	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 (QA) Plan;

e. Latest Individual Plant Examination for External Events/Probabilistic Risk Assessment Report; and
f. Vendor Manuals.

(2) Assessment and Corrective Actions:

a. The most recent Cyber-Security 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 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.