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

December 31, 2018

Mr. Eric Larson, Site Vice President
Entergy Operations, Inc.
Grand Gulf Nuclear Station
P.O. Box 756
Port Gibson, MS 39150

SUBJECT: GRAND GULF NUCLEAR STATION, UNIT 1 – NOTIFICATION OF CYBER SECURITY INSPECTION (05000416/2019410) AND REQUEST FOR INFORMATION

Dear Mr. Larson:

On April 29, 2019, the U.S. Nuclear Regulatory Commission (NRC) will begin an inspection in accordance with Inspection Procedure (IP) 71130.10P, "Cyber Security," Revision 0, at the Grand Gulf Nuclear Station. This inspection evaluates and verifies your ability to meet the full implementation 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." The onsite portion of the inspection will take place during the weeks of April 29 and May 13, 2019.

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, we have enclosed a request for documents needed for the inspection. The document request has been divided into four groups. The first group specifies information necessary to assist the team in choosing the focus areas (i.e., "sample set") to be inspected in accordance with the cyber security inspection procedure. This information should be made available using passive media (i.e. CD, DVD) and delivered to the regional office no later than March 1, 2019. The inspection team will review this information and by the end of the planned information gathering visit, March 21, 2019, will identify the specific items that should be provided for review.

The second group of requested documents will assist the team in their evaluation of the critical systems and critical digital assets, defensive architecture, and the areas of the cyber security plan selected for inspection. This information will be requested for review in the regional office prior to the inspection by April 5, 2019.

The third group of requested documents consists of those items that the team will review or need access to, during the inspection. Please have this information available by the first day of the onsite inspection, April 29, 2019.

The fourth group of information is necessary to aid the 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 Nnaerika Okonkwo. We understand that our regulatory contact for this inspection is Sheryl Sweet. If there are any questions about the inspection or the material requested, please contact the lead inspector at 817-200-1114 or by e-mail at Nnaerika.Okonkwo@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 under 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 James Drake for/***

Gregory. E. Werner, Chief
Engineering Branch 2
Division of Reactor Safety

Docket No. 50-416
License No. NPF-29

Enclosure:
Request for Information –
Cyber Security Inspection Document

cc: w/ encl: Electronic Distribution

**Request for Information – Cyber Security Inspection Document**
**Grand Gulf Nuclear Station, Unit 1**

| | |
|---|---|
| **Inspection Report:** | 05000416/2019410 |
| **Inspection Dates:** | Weeks of April 29, 2019, and May 13, 2019 |
| **Inspection Procedure:** | IP 71130.10P, "Cyber Security," Revision 0 |
| **Reference 1:** | ML17156A215 - "Guidance Document for Development of the Request for Information (RFI) and Notification Letter for Full-Implementation of the Cyber Security Inspection," Revision 1, dated October 26, 2017 |


| | | |
|---|---|---|
| **NRC Inspectors:** | Nnaerika Okonkwo, Lead<br>817-200-1114<br>Nnaerika.Okonkwo@nrc.gov | Greg Pick,<br>817-200-1270<br>Greg.Pick@nrc.gov |
| **NRC Contractors:** | Alan Konkal<br>561-859-5232<br>Alan.Konkal@nrc.gov | Alexander Prada<br>240-449-5791<br>Alexander.Prada@nrc.gov |


## *I. Information Requested for In-Office Preparation*

The initial request for information (i.e., first RFI) provides the team with the general information necessary to select appropriate components and cyber security plan elements to develop a site-specific inspection plan. The team will use the first set of information requested to identify the list of critical systems and critical digital assets plus operational and management security control portions of the Cyber Security Plan to be chosen as the "sample set" required to be inspected during this inspection. The first information request is specified in Table RFI #1.

The required Table RFI #1 information shall be provided on passive media (i.e. CD or DVD) to the lead inspector by March 1, 2019, or sooner to facilitate the selection of the specific items that will be reviewed during the onsite inspection weeks. Please provide four copies of each media submitted (i.e., one for each inspector/contractor). The preferred file format for all lists is a searchable Excel spreadsheet file on a CD or DVD. The files should be indexed and hyperlinked to facilitate efficient review. If you have any questions regarding this information, please contact the inspection team lead as soon as possible.

Table RFI #1

| Par No. | Section 3: Initial Documentation Requests (See Reference 1) Number/Title: | Items |
|---|---|---|
| 1 | List all identified critical systems and critical digital assets | All |
| 2 | List critical digital asset facility and site ethernet – transmission control protocol/internet protocol (TCP/IP) based local area networks (LANs) and identify those LAN's that have non-critical digital assets on them | All |

| Table RFI #1 | | |
|---|---|---|
| **Par No.** | **Section 3: Initial Documentation Requests (See Reference 1) Number/Title:** | **Items** |
| 3 | List critical digital asset facility and site non-ethernet TCP/IP based LANs including those industrial networks and identify LANs that have non-critical digital assets on them | All |
| 4 | Network topology diagrams (be sure to include all network intrusion detection systems and security information and event management (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 critical digital asset wireless Industrial networks | All |
| 11 | Network Intrusion detection system documentation for critical systems that have critical digital assets associated with them | 11.a.1)<br>11.a.2) |
| 12 | SIEM documentation for critical systems that have critical digital assets associated with them | 12.a.1)<br>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 any 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 provide the following:

(1) Electronic copy of the updated safety analysis report and technical specifications
(2) Name(s) and phone number(s) for the regulatory and technical contacts
(3) Current management and engineering organizational charts
(4) Cyber Security Program Procedures

Based on this information, the team will identify and select specific systems and equipment (e.g., critical systems and critical digital assets) from the information requested by Table RFI #1, and submit a list of specific systems and equipment to your staff by the end of the information gathering visit, March 21, 2019, for the second information request (i.e., Table RFI #2).

## *II. Additional Information Requested to be Available Prior to Inspection*

As stated in Section I, the team will examine the documents from the initial information request, and submit the list of specific systems and equipment to your staff by the end of the information gathering visit, March 21, 2019. This second information request (i.e., Table RFI #2) obtains additional documents required to evaluate the critical systems and critical digital assets, defensive architecture, and the areas of the cyber security program 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 Reference 1.

The Table RFI #2 information shall be provided on passive media to the lead inspector by April 5, 2019. Please provide four copies of each CD/DVD submitted (i.e., one for each inspector/contractor). The preferred file format for all lists is a searchable Excel spreadsheet file on a CD/DVD. These passive media should be indexed and hyperlinked to facilitate efficient review. If you have any questions regarding this information, please call the inspection team lead as soon as possible.

Table RFI #2

| Par No. | Section 3: Initial Documentation Requests (See Reference 1) 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 | Block diagrams for distributed systems (for systems selected for inspection) | All |
| 10 | Host-based intrusion detection system documentation for critical digital assets (for systems selected for inspection) | 10.a.1)<br>10.a.2) |
| 13 | List all maintenance and test equipment (M&TE) used on critical digital assets (for systems selected for inspection) | All |
| 15 | Configuration management | All |
| 11 | Network Intrusion detection system documentation for critical systems that have critical digital assets associated with them | 11.a.1)<br>11.a.2) |
| 16 | Supply chain management | 16.a<br>16.b |
| 17 | Portable media and mobile device control | All |
| 18 | Software management | All |

| Table RFI #2 | | |
|---|---|---|
| **Par No.** | **Section 3: Initial Documentation Requests (See Reference 1) Number/Title:** | **Items** |
| 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 NRC 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 Section II, provide the following request for information (i.e., Table 1st Week Onsite) on passive media by April 29, 2019, the first day of the inspection. All requested information shall follow the guidance in Reference 1.

Please provide four copies of each CD submitted (i.e., one for each inspector/contactor). The preferred file format for all lists is a searchable Excel spreadsheet file on a CD/DVD. These passive media files should be indexed and hyperlinked to facilitate ease of use. If you have any questions regarding this information, please call the inspection team lead as soon as possible.

| Table 1st Week Onsite | | |
|---|---|---|
| **Par No.** | **Section 3: Initial Documentation Requests (See Reference 1) Number/Title:** | **Items** |
| 10 | Host-based intrusion detection system documentation for critical digital assets (for systems selected for inspection) | 10.a.3) thru 10.a.12) |
| 11 | Network Intrusion detection system documentation for critical systems that have critical digital assets associated with them | 11.a.3) thru 11.a.15) |
| 12 | SIEM documentation for critical systems that have critical digital assets associated with them | 12.a.3) thru 12.a.14 |
| 16 | Supply chain management | 16.c |

| Table 1st Week Onsite | | |
|---|---|---|
| **Par No.** | **Section 3: Initial Documentation Requests (See Reference 1) Number/Title:** | **Items** |
| 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. Quality Assurance Plan;

b. Technical Specifications, if not previously provided;

c. Latest Individual Plant Examination/Probabilistic Risk Assessment Report; and,

(2) Vendor Manuals, Assessments, 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 team lead.

GRAND GULF NUCLEAR STATION, UNIT 1 – NOTIFICATION OF CYBER SECURITY INSPECTION (05000416/2019410) AND REQUEST FOR INFORMATION – DECEMBER 31, 2018

**DISTRIBUTION:**
KKennedy, ORA
SMorris, ORA
TVegel, DRP
MHay, DRP
MShaffer, DRS
RLantz, DRS
TSteadham, DRP
NDay, DRP
JKozal, DRP
CYoung, DRP
DProulx, DRP
AElam, DRP
RRemigio, DRP
VDricks, ORA
SLingam, NRR
GMiller, DRS
PJayroe, DRS
MHerrera, DRMA
R4Enforcement
DCylkowski, ORA
JWeil, OWFN
AMoreno, OWFN
CCook, OEDO
BMaier, ORA

ADAMS ACCESSION NUMBER: ML19003A381

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

| OFFICE | RI:EB2 | BC:EB2 | | | | |
|---|---|---|---|---|---|---|
| NAME | N. Okonkwo | G. Werner | | | | |
| SIGNATURE | ***/RA-e/*** | ***/RA JFD for/*** | | | | |
| DATE | ***12/27/2018*** | ***12/31/2018*** | | | | |

**OFFICIAL RECORD COPY**