



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

January 10, 2018

Mr. William F. Maguire, Vice President  
Entergy Operations, Inc.  
River Bend Station  
5485 US Highway 61N  
St. Francisville, LA 70775

SUBJECT: RIVER BEND STATION – NOTIFICATION OF CYBER SECURITY  
INSPECTION (NRC INSPECTION REPORT 05000458/2018406) AND  
REQUEST FOR INFORMATION

Dear Mr. Maguire:

On May 7, 2018, 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 River Bend 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 May 7, 2018, and May 21, 2018.

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 26, 2018. The inspection team will review this information and by the end of the planned information gathering visit on April 12, 2018, will request 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 23, 2018, as identified above.

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, May 7, 2018.

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 Sam Graves. We understand that our regulatory contact for this inspection is Bridget Johns. If there are any questions about the inspection or the material requested, please contact the lead inspector at 817-200-1102 or by e-mail at [samuel.graves@nrc.gov](mailto:samuel.graves@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/*

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

Docket No. 50-458  
License No. NPF-47

Enclosure:  
River Bend Station –  
Cyber Security Inspection Document Request

cc w/ encl: Electronic Distribution

## **River Bend Station – Cyber Security Inspection Document Request**

**Inspection Report:** 05000458/2018406

**Inspection Dates:** Weeks of May 7, 2018, and May 21, 2018

**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:**

Samuel Graves, Lead 817-200-1102 <a href="mailto:samuel.graves@nrc.gov">samuel.graves@nrc.gov</a>	Eduardo Uribe 817-200-1534 <a href="mailto:eduardo.uribe@nrc.gov">eduardo.uribe@nrc.gov</a>
Steve Alferink (Observer) 817-200-1548 <a href="mailto:steven.alferink@nrc.gov">steven.alferink@nrc.gov</a>	

**NRC Contractors:**

Casey Priester <a href="mailto:frederick.priester@nrc.gov">frederick.priester@nrc.gov</a>	William Johns <a href="mailto:william.johns@nrc.gov">william.johns@nrc.gov</a>
--	---

### **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 (CSs) and critical digital assets (CDAs) 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. Provide the first set of information to the team leader in the regional office by March 26, 2018, or sooner, to facilitate the selection of the specific items that will be reviewed during the onsite inspection weeks.

The team will examine the returned documentation from the first information request and select specific systems and equipment (e.g., CSs/CDAs) to provide a more focused follow-up RFI to develop the second information request. The team will submit the second information request to your staff by the end of the planned information gathering visit on April 12, 2018, which will identify the specific systems and equipment that will be utilized to evaluate the CSs and CSAs, defensive architecture, and the areas of the cyber security program selected for the cyber security inspection. We request that the additional information provided from the second RFI be made available to the regional office prior to the inspection, if possible, but no later than the first day of onsite inspection. All requests for information shall follow the guidance in Reference 1.

Enclosure

The required Table RFI #1 information shall be provided on passive media (i.e. CD or DVD) to the lead inspector by March 26, 2018. 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 leader as soon as possible.

Table RFI #1		
<b>Section 3: Initial Documentation Requests (See Reference 1)</b>		<b>Items</b>
<b>Paragraph Number/Title:</b>		
1	List All Identified Critical Systems and Critical Digital Assets	All
2	List CDA Facility and Site Ethernet – Transmission Control Protocol/Internet Protocol (TCP/IP) based Local Area Networks (LANs) and identify those LAN's that have non-CDAs on them	All
3	List CDA facility and site non-Ethernet TCP/IP 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 Systems 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	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 any 50.54(p) analysis to support changes to that plan	All
29	Copy of any Licensee Identified Violations (LIVs) and associated Corrective Action Program (CAP) 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 (USAR) and technical specifications
- (2) Name(s) and phone number(s) for the regulatory and technical contacts
- (3) Current management and engineering organizational charts

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 on April 12, 2018, 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 above, the team will examine the returned documentation requested 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 on April 12, 2018, for the second RFI (i.e., Table RFI #2). This second information request obtains additional documents required to evaluate the CSs and CSAs, 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 23, 2018. 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 leader as soon as possible.

Table RFI #2		
<b>Section 3: Initial Documentation Requests (See Reference 1)</b>		
<b>Paragraph Number/Title:</b>		<b>Items</b>
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 CDAs (for systems selected for inspection)	10.a.1) 10.a.2)
13	List all Maintenance and Test Equipment (M&TE) 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
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

Table RFI #2	
Section 3: Initial Documentation Requests (See Reference 1) Paragraph Number/Title:	Items
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 above, provide the following RFI (i.e., Table 1<sup>st</sup> Week Onsite) on passive media by May 7, 2018, the first day of the inspection. All requested information shall follow the guidance in Reference 1.

Please provide five 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 leader as soon as possible.

Table 1 <sup>st</sup> Week Onsite	
Section 3: Initial Documentation Requests (See Reference 1) 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.b.2) 16.b.3) 16.b.4)
19 Cyber Security Event Notifications	All
29 Update to LIV's and CAP 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 leader.

RIVER BEND STATION – NOTIFICATION OF CYBER SECURITY INSPECTION  
(NRC INSPECTION REPORT 05000458/2018406) AND REQUEST FOR INFORMATION -  
JANUARY 10, 2018

**Electronic distribution by RIV:**

KKennedy, ORA  
SMorris, ORA  
TPruett, DRP  
RLantz, DRP  
AVegel, DRS  
JClark, DRS  
JSowa, DRP  
BParks, DRP  
JKozal, DRP  
CYoung, DRP  
TDeBey, DRP  
LDay, DRP  
VDricks, ORA  
LRegner, NRR  
THipschman, DRS  
EUribe, DRS  
MHerrera, DRMA  
R4Enforcement  
SKirkwood, OGC  
JWeil, OWFN  
AMoreno, OWFN  
JBowen, OEDO  
BMaier, ORA

ADAMS ACCESSION NUMBER: ML18011A046

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

OFFICE	SRI:EB2	BC:EB2				
NAME	S. Graves	G. Werner				
SIGNATURE	/RA/	/RA/				
DATE	01/09/2017	01/10/2017				

OFFICIAL RECORD COPY