UNITED STATES
NUCLEAR REGULATORY COMMISSION
REGION II
245 PEACHTREE CENTER AVENUE N.E., SUITE 1200
ATLANTA, GEORGIA 30303-1200

January 26, 2024

Jamie M. Coleman
Regulatory Affairs Director
Southern Nuclear Operating Co., Inc.
3535 Colonnade Parkway
Birmingham, AL 35243

SUBJECT: VOGTLE ELECTRIC GENERATING PLANT - INFORMATION REQUEST FOR THE CYBER-SECURITY BASELINE INSPECTION, NOTIFICATION TO PERFORM INSPECTION 05000424/2024403; 05000425/2024403

Dear Jamie Coleman:

On March 25, 2024, the U.S. Nuclear Regulatory Commission (NRC) will begin a baseline inspection in accordance with Inspection Procedure (IP) 71130.10 “Cyber-Security,” Revision 0 at your Vogtle Electric Generating Plant, Units 1 and 2. The inspection will be performed to evaluate and verify your ability to provide assurance that your digital computer and communication systems and networks associated with safety, security, or emergency preparedness (SSEP) functions are adequately protected against cyber-attacks in accordance with Title 10 of the Code of Federal Regulations (10 CFR) 73.54 and the U.S. Nuclear Regulatory Commission (NRC) approved cyber security plan (CSP). The onsite portion of the inspection will take place during the week of March 25th, 2024.

Experience has shown that baseline inspections are extremely resource intensive, both for the NRC inspectors and the 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 cyber-security IP. This information should be made available electronically no later than February 9, 2024. The inspection team will review this information and, by February 16, 2024, will request the specific items that should be provided for review. This second group of additional 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 the licensee’s CSP selected for the cyber-security inspection. We request that the information provided from the second RFI be made available to the regional office prior to the inspection by March 15, 2024.

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, March 25, 2024.

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 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 Philipp Braaten. We understand that our regulatory contact for this inspection is Jamaal Merriweather 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.

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.

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).

Sincerely,

Daniel M. Bacon Signed by Bacon, Daniel on 01/26/24

Daniel Bacon, Chief
Engineering Branch 2
Division of Reactor Safety

Docket Nos. 50-424; 50-425
License Nos. NPF-68; NPF-81

Enclosure:
Vogtle Electric Generating Plant Cyber-Security Inspection Document Request

cc w/encl: Distribution via LISTSERV®

SUBJECT: VOGTLE ELECTRIC GENERATING PLANT - INFORMATION REQUEST FOR THE CYBER-SECURITY BASELINE INSPECTION, NOTIFICATION TO PERFORM INSPECTION 05000424/2024403; 05000425/2024403 DATED JANUARY 26, 2024

**DISTRIBUTION:**
P. Braaten, RII
D. Strickland, RII
A. Blamey, RII
A. Alen, RII
C. Scott, RII
T. Morrissey, RII

ADAMS ACCESSION NUMBER: **ML24018A189**

| ☒ SUNSI Review | | ☒ Non-Sensitive<br>☐ Sensitive | | ☒ Publicly Available<br>☐ Non-Publicly Available | |
|---|---|---|---|---|---|
| OFFICE | RII/DRS | RII/DRS | | | |
| NAME | P. Braaten | D. Bacon | | | |
| DATE | 01/25/2024 | 01/26/2024 | | | |

**OFFICIAL RECORD COPY**

**VOGTLE ELECTRIC GENERATING PLANT CYBER-SECURITY INSPECTION DOCUMENT REQUEST**

**Inspection Report:** 05000424/2024403; 05000425/2024403

**Inspection Dates:** March 25 – March 29, 2024

**Inspection Procedure:** IP 71130.10, "Cyber-Security," Revision 0 (Effective: 01/01/2022)

**Reference:** "Guidance Document for Development of the Request for Information (RFI) and Notification Letter for Full-Implementation of the Cyber-Security Inspection," Rev. 2 (Issued: 11/22/2021)

**NRC Inspectors:**

Philipp Braaten, Lead
404-997-4651
philipp.braaten@nrc.gov

David Strickland
404-997-4440
David.strickland@nrc.gov

Jeff Rady
301-415-5097
Jeff.rady@nrc.gov

**NRC Contractors:**

Balla Barro
balla.barro@nrc.gov

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

The initial request for information (i.e., first RFI) concentrates on providing the inspection team with the general information necessary to select appropriate components and 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 (O&M) security control portions of the CSP to be chosen as the "sample set" required to be inspected by the cyber-security IP. 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 **February 9, 2024**, 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 **February 16, 2024**, 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.

**VOGTLE ELECTRIC GENERATING PLANT CYBER-SECURITY INSPECTION DOCUMENT REQUEST**

We request that the additional information provided from the second RFI be made available to the regional office prior to the inspection by **March 15, 2024**. All requests for information shall follow the guidance document U.S. NRC - Guidance Document for Development of the Request for Information (RFI) and Notification Letter for Full Implementation of the Cyber-Security Inspection, referenced above.

**VOGTLE ELECTRIC GENERATING PLANT CYBER-SECURITY INSPECTION DOCUMENT REQUEST**

The required Table RFI 1 information shall be provided electronically to the lead inspector by **February 9, 2024**. 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 call the inspection team leader as soon as possible.

| Table RFI #1 | | |
|---|---|---|
| **Paragraph Number/Title:** | | **IP Ref** |
| 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 | 03.03(a) |

| Table RFI #1 | | |
|---|---|---|
| **Paragraph Number/Title:** | | **IP Ref** |
| | inspection, including either a summary of the design change or the 50.59 documentation for the change. | |
| 13 | Supply Chain Management program documentation including a list of security impact analysis for new acquisitions. | 03.03(a), (b) and (c) |
| 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 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 | Any cyber security event reports submitted in accordance with 10 CFR 73.77 since the last cyber security inspection and any copies of any **recordable** cyber security events since the last inspection | 03.04(a) |

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 **February 16, 2024** 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 **February 16, 2024** 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 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 referenced above.

The Table RFI 2 information shall be provided to the lead inspector by **March 15, 2024**. The preferred file format for all lists is a searchable Excel spreadsheet. The information

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 | | |
|---|---|---|
| **Paragraph Number/Title:** | | **Items** |
| | **For the system(s) chosen for inspection provide:** | |
| 1 | Ongoing Monitoring and Assessment activity performed on the selected system(s). | 03.01(a) |
| 2 | All Security Control Assessments for the selected design changes and 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.* All vulnerability screenings and assessments completed prior to putting new equipment into service as part of the select design changes. | 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 and for selected design changes. * | 03.03(a) |
| 8 | Security impact analysis for the selected design changes. | 03.03(b) |
| 9 | Copies of the purchase order documentation for selected design changes. | 03.03(c) |
| 10 | Copies of any reports/assessment for cyber security drills performed since the last inspection. | 03.02(a)<br>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)<br>03.04(b) |

| Table RFI #2 | | |
|---|---|---|
| **Paragraph Number/Title:** | | **Items** |
| 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.*

## *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 Week Onsite) to the team by March 25, 2024, 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 call the inspection team leader as soon as possible.

| Table Week Onsite | | |
|---|---|---|
| **Paragraph Number/Title:** | | **Items** |
| 1 | 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 |
| 2 | The most recent Cyber-Security Quality Assurance audit and/or self-assessment and a list of Corrective Actions generated as a result | |

## *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.