UNITED STATES
NUCLEAR REGULATORY COMMISSION
REGION I
475 ALLENDALE RD, STE 102
KING OF PRUSSIA, PENNSYLVANIA 19406-1415

July 29, 2025

David P. Rhoades
Senior Vice President
Constellation Energy Generation, LLC
President and Chief Nuclear Officer (CNO)
Constellation Nuclear
4300 Winfield Road
Warrenville, IL 60555

SUBJECT: LIMERICK GENERATING STATION, UNITS 1 AND 2 – INFORMATION REQUEST FOR THE CYBERSECURITY BASELINE INSPECTION, NOTIFICATION TO PERFORM INSPECTION 05000352/2025403 AND 05000353/2025403

Dear David Rhoades:

On December 8, 2025, the U.S. Nuclear Regulatory Commission (NRC) will begin a baseline inspection in accordance with Inspection Procedure (IP) 71130.10, "Cyber Security," dated December 14, 2021, at your Limerick Generating Station, Units 1 and 2. The inspection will be performed to evaluate and verify your ability to meet the requirements of the NRC's Cyber Security Rule, Title 10 of the *Code of Federal Regulations* (10 CFR) Part 73, Section 54, "Protection of Digital Computer and Communication Systems and Networks." The onsite portion of the inspection will take place December 8–12, 2025.

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 IP 71130.10. This information should be made available either on an online repository (preferred) or digital media (CD/DVD) no later than September 5, 2025. The inspection team will review this information and, by October 3, 2025, 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 the licensee's cybersecurity program selected for the cybersecurity inspection. This information will be requested for review in the regional office prior to the inspection by October 31, 2025, as identified above.

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, December 8, 2025.

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 En De Chen. We understand that our regulatory contact for this inspection is Jordan Rajan of your organization. If there are any questions about the inspection or the material requested, please contact the lead inspector at (610) 337-5136 or via email at En.Chen@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 component of the NRC's Agencywide Documents Access and Management System (ADAMS). ADAMS is accessible from the NRC website at http://www.nrc.gov/reading-rm/adams.html (the Public Electronic Reading Room).

Sincerely,

GLENN
DENTEL

Digitally signed by
GLENN DENTEL
Date: 2025.07.29
07:00:24 -04'00'

Glenn T. Dentel, Chief
Engineering Branch 2
Division of Operating Reactor Safety

Docket Nos. 05000352 and 05000353
License Nos. NPF-39 and NPF-85

Enclosure:
Cybersecurity Inspection Document Request

cc: Distribution via ListServ

SUBJECT: LIMERICK GENERATING STATION, UNITS 1 AND 2 – INFORMATION REQUEST FOR THE CYBERSECURITY BASELINE INSPECTION, NOTIFICATION TO PERFORM INSPECTION 05000352/2025403 AND 05000353/2025403 DATED JULY 29, 2025

DISTRIBUTION:
GDentel, DORS
EChen, DORS
NWarnek, DORS
RClagg, DORS
BKwiatkowski, DORS
BFord, DORS
AZiedonis, DORS, SRI
LGrimes, DORS, RI
TSteadham, RI OEDO
RidsNrrPMLimerick Resource
RidsNrrDorlLpl1 Resource
R1ORAMAIL Resource

DOCUMENT NAME: https://usnrc.sharepoint.com/teams/EngineeringBranch2/Shared Documents/_Cyber Security/_Baseline Inspections - OUO_SRI/2025/Limerick/RFI Letter/Limerick Cybersecurity 2025 RFI 1.docx
ADAMS ACCESSION NUMBER: ML25210A012

☑ SUNSI Review		☑ Non-Sensitive □ Sensitive		☑ Publicly Available □ Non-Publicly Available	
OFFICE	RI/DORS	RI/DORS			
NAME	EChen	GDentel			
DATE	7/28/2025	7/28/2025			

OFFICIAL RECORD COPY

LIMERICK CYBERSECURITY INSPECTION DOCUMENT REQUEST

Inspection Report:	05000352/2025403 and 05000353/2025403	
Inspection Dates:	December 8 to December 12, 2025	
Inspection Procedure:	Inspection Procedure (IP) 71130.10, “Cyber Security,” dated December 14, 2021 (ADAMS Accession Number: ML21271A106)	
Reference:	Guidance Document for Development of the Request for Information (RFI) and Notification Letter for IP 71130.10, “Cyber Security” (ML21330A088)	
NRC Inspectors:	En De Chen, Lead (610) 337-5136 En.Chen@nrc.gov	Joseph Cunningham (610) 337-5390 Joseph.Cunningham@nrc.gov
NRC Contractors:	Timothy Hennessey (610) 337-5135 Timothy.Hennessey@nrc.gov	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 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 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 September 5, 2025, 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 October 3, 2025, 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. We request that the additional information provided from the second RFI be made available to the regional office prior to the inspection by October 31, 2025.

Enclosure

LIMERICK CYBERSECURITY INSPECTION DOCUMENT REQUEST

The required Table RFI 1 information shall be provided on an online repository (preferred) or digital media (CD/DVD) to the lead inspector by September 5, 2025. The preferred file format for all lists is a searchable Excel spreadsheet file. The information 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 RFI #1		
Section 3, Paragraph Number/Title:		**IP Ref**
1	A list of all Identified Critical Systems and Critical Digital Assets – highlight/note any additions, deletions or 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 emergency preparedness 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 and the most recent cybersecurity Quality Assurance audit/assessment. Please include any condition reports (or similar) generated as a result of the audits/assessments.	03.01(b)
6	Vulnerability screening/assessment and scan program documentation.	03.01(c)
7	Device Access and Key Control program documentation.	03.02(c)
8	Password/Authenticator documentation.	03.02(c)
9	User Account/Credential program documentation.	03.02(d)
10	Portable Media and Mobile Device control program documentation, including kiosk security control assessment/documentation.	03.02(e)
11	Design change/modification program documentation and a list of all design changes completed since the last two cyber security inspections, including either a summary of the design change or the 50.59 documentation for the change. Please notate/highlight which design changes affected Critical Digital Assets (added, modified, deleted, etc.)	03.03(a)
12	Supply Chain Management documentation including any security impact analysis for new acquisitions.	03.03(a), (b) and (c)
13	Configuration Management documentation including any security impact analysis performed due to configuration changes since the last inspection.	03.03(a) and (b)
14	Cyber Security Metrics tracked (if applicable).	03.06 (b)
15	Provide documentation describing any cyber security changes to the access authorization program since the last cyber security inspection.	Overall
16	Provide a list of all procedures and policies provided to the NRC as part of this RFI with their descriptive name and associated number (if available).	Overall
17	Performance testing report (if applicable).	03.06 (a)
18	List of Condition Reports (or similar) associated with cybersecurity issues written since the last inspection. Please include CR #, date written, and a short description / title.	Overall

In addition to the above information please provide the following:

(1) Name(s) and phone numbers for the regulatory and technical contacts.

(2) 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 October 3, 2025, 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 October 3, 2025, 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.

The Table RFI #2 information shall be provided to the lead inspector by October 31, 2025. The preferred file format for all lists is a searchable Excel spreadsheet. The information 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 RFI #2		
Section 3, Paragraph Number/Title:		**Items**
	For the systems and CDAs chosen for inspection provide:	
1	Ongoing Monitoring and Assessment activity performed on the system(s).	03.01(a)
2	All Security Control Assessments for the selected 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.	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 inspection.	03.02(d)
7	Baseline configuration data sheets for the selected CDAs.	03.03(a)
8	Documentation on any changes, including Security Impact Analyses, performed on the selected system(s) since the last inspection.	03.03(b)

Table RFI #2

Section 3, Paragraph Number/Title:		**Items**
9	Copies of the purchase order documentation for any new equipment purchased for the selected systems since the last inspection.	03.03(c)
10	For the selected systems, provide design change/modification packages including completed work orders since the last cyber security inspection.	03.03(a)

III. *Information Requested to be Available on First Day of Inspection*

Please provide the following information to the team by December 8, 2025, the first day of the inspection.

Table 1ST Week Onsite

Section 3, Paragraph Number/Title:		**Items**
1	Updated list of corrective actions that were generated since the corrective actions provided for RFI #2, to include any corrective actions generated as a result of self assessments performed prior to the inspection.	03.01b

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.