



UNITED STATES
NUCLEAR REGULATORY COMMISSION
WASHINGTON, D.C. 20555-0001

May 21, 2010

Christopher L. Burton, Vice President
Shearon Harris Nuclear Power Plant
Carolina Power & Light Company
Post Office Box 165, Mail Zone 1
New Hill, North Carolina 27562-0165

SUBJECT: SHEARON HARRIS NUCLEAR POWER PLANT, UNIT 1—INITIAL REVIEW
REGARDING THE LICENSE AMENDMENT REQUEST FOR APPROVAL OF
THE CYBER SECURITY PLAN (TAC NO. ME2796)

Dear Mr. Burton:

By letter dated November 19, 2009, (Agencywide Documents Access and Management System (ADAMS) Accession No. ML093290248), Carolina Power & Light Company (CP&L), now doing business as Progress Energy Carolinas, Inc., submitted a license amendment request (LAR) for the Shearon Harris Nuclear Power Plant, Unit 1 (HNP). The proposed LAR includes the cyber security plan, proposed changes to paragraph 2.E of the renewed facility operating license, and a proposed cyber security plan implementation schedule. The proposed cyber security plan has been submitted in accordance with Title 10 of the *Code of Federal Regulations* (10 CFR), Section 73.54, "Protection of digital computer and communication systems and networks."

The purpose of this letter is to inform you that the U.S. Nuclear Regulatory Commission (NRC) staff has completed an initial review of this LAR. In accordance with the Office of Nuclear Reactor Regulation Office Instruction LIC-109, "Acceptance Review Procedures" (ADAMS Accession No. ML091810088), Section 3.1.3, "Rare Circumstances," the NRC staff has decided to forgo the traditional acceptance review due to the complexity and "first-of-a-kind" nature of this application. While the NRC staff has docketed your application, we are not rendering a judgment as to the acceptability of the submittal within the context of an acceptance review.

The cyber security plan submittal prepared for HNP is based on the Nuclear Energy Institute (NEI) guidance contained in NEI 08-09, "Cyber Security Plan for Nuclear Power Reactors," Revision 3. The NRC staff had significant generic concerns with the earlier versions of this guidance. As a result of NRC staff discussions with NEI and the Executive Task Force of the industry Nuclear Security Working Group (NSWG), NEI and NSWG committed to representing operating power reactor licensees in resolving these concerns.

Through numerous interactions, the NRC staff has communicated its generic concerns with the NEI guidance. The security-related nature of the information required these interactions to be conducted in closed meetings not open to the public. A publicly available list of the specific issues discussed with NEI and NSWG was communicated to the licensees via e-mail dated March 9, 2010 (ADAMS Accession No. ML100680284).

By letter dated April 28, 2010, NEI submitted Revision 6 to NEI 08-09 (ADAMS Accession Nos. ML101180434 and ML101180437), which contains changes that address the NRC staff concerns associated with previous versions. Based on a technical review of the document, the

Office of Nuclear Security and Incident Response, in its letter dated May 5, 2010 (ADAMS Accession No. ML101190371), concluded that submission of a cyber security plan using the template provided in NEI 08-09, Revision 6, dated April 2010, would be an acceptable means for licensees to demonstrate compliance with the requirements of 10 CFR 73.54, with the exception of the definition of "cyber attack."

Therefore, to resolve the NRC staff's concerns with the requested LAR, CP&L is requested to review the list of generic issues provided to the industry cyber security writing team and forwarded to all licensees via e-mail dated March 9, 2010, and provide a revised submittal as appropriate. For those generic issues that will not be addressed in the revised submittal, please provide additional information or justification in the revised submittal to discuss their exclusion.

For any changes to the cyber security plan proposed in the original LAR, CP&L is requested to indicate that the revised submittal supersedes, in its entirety, the previous submittal (or indicate what portions are superseded).

As an alternative to, and a potentially less resource intensive method than, addressing the individual generic issues within the existing submittal, CP&L may submit a revised cyber security plan consistent with Regulatory Guide 5.71¹ or submit a revised cyber security plan consistent with NEI 08-09, Revision 6. However, if this option is exercised, the NRC staff expects that the existing application will be withdrawn and the revised application resubmitted concurrently.

The NRC staff requests that CP&L's response or revised cyber security plan application be submitted within 60 days of the date of this letter. Please contact me if circumstances result in the need to revise the requested response date.

Following receipt and review of your response, you will be advised by separate correspondence if any further information is needed to support the NRC staff's detailed technical review. If you have any questions regarding this matter, I may be reached at (301) 415-3178.

Sincerely,



Marlayna Vaaler, Project Manager
Plant Licensing Branch II-2
Division of Operating Reactor Licensing
Office of Nuclear Reactor Regulation

Docket No. 50-400

cc: Distribution via ListServ

¹ In January 2010, the NRC staff issued RG 5.71, "Cyber Security Programs for Nuclear Facilities" (ADAMS Accession No. ML090340159). This guidance provides an approach that the NRC staff deems acceptable for complying with the Commission's regulations regarding the protection of digital computers, communications systems, and networks from a cyber security attack.

Office of Nuclear Security and Incident Response, in its letter dated May 5, 2010 (ADAMS Accession No. ML101190371), concluded that submission of a cyber security plan using the template provided in NEI 08-09, Revision 6, dated April 2010, would be an acceptable means for licensees to demonstrate compliance with the requirements of 10 CFR 73.54, with the exception of the definition of "cyber attack."

Therefore, to resolve the NRC staff's concerns with the requested LAR, CP&L is requested to review the list of generic issues provided to the industry cyber security writing team and forwarded to all licensees via e-mail dated March 9, 2010, and provide a revised submittal as appropriate. For those generic issues that will not be addressed in the revised submittal, please provide additional information or justification in the revised submittal to discuss their exclusion.

For any changes to the cyber security plan proposed in the original LAR, CP&L is requested to indicate that the revised submittal supersedes, in its entirety, the previous submittal (or indicate what portions are superseded).

As an alternative to, and a potentially less resource intensive method than, addressing the individual generic issues within the existing submittal, CP&L may submit a revised cyber security plan consistent with Regulatory Guide 5.71¹ or submit a revised cyber security plan consistent with NEI 08-09, Revision 6. However, if this option is exercised, the NRC staff expects that the existing application will be withdrawn and the revised application resubmitted concurrently.

The NRC staff requests that CP&L's response or revised cyber security plan application be submitted within 60 days of the date of this letter. Please contact me if circumstances result in the need to revise the requested response date.

Following receipt and review of your response, you will be advised by separate correspondence if any further information is needed to support the NRC staff's detailed technical review. If you have any questions regarding this matter, I may be reached at (301) 415-3178.

Sincerely,
/RA/
Marlayna Vaaler, Project Manager
Plant Licensing Branch II-2
Division of Operating Reactor Licensing
Office of Nuclear Reactor Regulation

Docket No. 50-400

cc: Distribution via ListServ

¹ In January 2010, the NRC staff issued RG 5.71, "Cyber Security Programs for Nuclear Facilities" (ADAMS Accession No. ML090340159). This guidance provides an approach that the NRC staff deems acceptable for complying with the Commission's regulations regarding the protection of digital computers, communications systems, and networks from a cyber security attack.

DISTRIBUTION:

PUBLIC LPL2-2 R/F	RidsAcrcsAcnw_MailCTR Resource	RidsOgcRp Resource
RidsNrrDirsltsb Resource	RidsNrrDorlDpr Resource	C. Erlanger, NSIR
RidsNrrDorlLpl2-2 Resource	RidsNrrPMHarris Resource	P. Pederson, NSIR
RidsNrrLACSola Resource	RidsRgn2MailCenter Resource	

ADAMS Accession No. ML101340167

OFFICE	LPL2-2/PM	LPL2-2/LA	LP2-2/BC
NAME	MVaaler	CSola	DBroaddus (S Bailey for)
DATE	05/19/10	05/17/10	05/21/10