



411 Fayetteville Street Mall
Raleigh NC 27602

10 CFR 50.4

Serial: RA-11-005

February 28, 2011

United States Nuclear Regulatory Commission
ATTENTION: Document Control Desk
Washington, DC 20555-0001

BRUNSWICK STEAM ELECTRIC PLANT, UNIT NOS. 1 AND 2
DOCKET NOS. 50-325 AND 50-324 / RENEWED LICENSE NOS. DPR-71 AND DPR-62

CRYSTAL RIVER UNIT 3 NUCLEAR GENERATING PLANT
DOCKET NO. 50-302 / LICENSE NO. DPR-72

SHEARON HARRIS NUCLEAR POWER PLANT, UNIT NO. 1
DOCKET NO. 50-400 / RENEWED LICENSE NO. NPF-63

H. B. ROBINSON STEAM ELECTRIC PLANT, UNIT NO. 2
DOCKET NO. 50-261 / RENEWED LICENSE NO. DPR-23

**RESPONSE TO REQUEST FOR ADDITIONAL INFORMATION ON THE
CAROLINA POWER AND LIGHT COMPANY AND FLORIDA POWER
CORPORATION CYBER SECURITY PLAN, REVISION 0**

Ladies and Gentlemen:

By letter dated July 8, 2010, Carolina Power & Light Company (CP&L), now doing business as Progress Energy Carolinas, Inc., and Florida Power Corporation (FPC), now doing business as Progress Energy Florida, Inc., submitted the fleet *Carolina Power and Light Company and Florida Power Corporation Cyber Security Plan* (ML101950043) for NRC review and approval.

A Request for Additional Information (RAI) was received via electronic correspondence on December 20, 2010, (ML110120041). The RAI was subsequently discussed with the NRC staff via teleconference on January 11, 2011, (ML110120023). CP&L and FPC's response to the RAI is attached.

The response to the first question describes a change that must be made to the *Carolina Power and Light Company and Florida Power Corporation Cyber Security Plan*. An updated *Carolina Power and Light Company and Florida Power Corporation Cyber Security Plan* will be submitted, by follow-up correspondence, incorporating this change along with other changes that address common industry issues regarding balance of plant equipment, records retention, and implementation schedules. The date of this follow-up correspondence is dependent upon final resolution of the common industry issues and the NRC staff's issuance of a common industry RAI.

No new regulatory commitments have been made in this letter.

SDD/A
NRR

If you have questions regarding this submittal, please contact Brian McCabe, Manager, Nuclear Regulatory Affairs, at (919) 546-4579.

I declare under the penalty of perjury that the foregoing is true and correct. Executed on February 28, 2011.

Sincerely,



Garry Miller
Vice President – Nuclear Engineering
Progress Energy, Inc.

DBM

Attachment: Response to Request for Additional Information on the *Carolina Power and Light Company and Florida Power Corporation Cyber Security Plan*, Revision 0.

cc USNRC Region II
USNRC Resident Inspector – BSEP, Unit Nos. 1 and 2
USNRC Resident Inspector – CR3
USNRC Resident Inspector – SHNPP, Unit No. 1
USNRC Resident Inspector – HBRSEP, Unit No. 2
F. Saba, NRR Project Manager – BSEP, Unit Nos. 1 and 2; CR3
B. Mozafari, NRR Project Manager – SHNPP, Unit No. 1; HBRSEP, Unit No. 2

Attachment

Response to Request for Additional Information on the *Carolina Power and Light Company and Florida Power Corporation Cyber Security Plan, Revision 0*

Response to Request for Additional Information on the *Carolina Power and Light Company and Florida Power Corporation Cyber Security Plan, Revision 0*

Cyber Security Plan (CSP) Section 4: Establishing, Implementing, and Maintaining the Cyber Security Program

RAI 1

RAI Title: Defense-in-Depth Protective Strategies – Restriction of one-way communications between levels

Title 10 of the Code of Federal Regulations (10 CFR) Section 73.54(c)(2) requires the licensee to apply and maintain defense-in-depth protective strategies to ensure the capability to detect, respond to, and recover from cyber attacks. Section 4.3, “Defense-in-Depth Protective Strategies,” of the licensee’s fleet CSP states in bullet nine “Communications initiated from CDAs [critical digital assets] within the lower-level plant computing network (Level 3) to CDAs within the higher-level plant computing network (Level 4) is restricted as described in engineering design documentation.”

Question:

Explain how one-way communications will be restricted between two different security levels/zones that will prevent any data transmission from the low security level to the higher security level.

Answer:

The ninth bullet in Section 4.3 will be revised as follows:

Communication initiated from CDAs within the lower-level plant computing network (Level 3) to CDAs within the higher-level plant computing network (Level 4) is ~~restricted as described in engineering design documentation~~ through the use of a firewall and network-based intrusion detection system.

RAI 2

RAI Title: Defense-in-Depth Protective Strategies – Restriction of bi-directional communications between levels

Section 73.54(c)(2) of 10 CFR requires the licensee to apply and maintain defense-in-depth protective strategies to ensure the capability to detect, respond to, and recover from cyber attacks. Section 4.3, “Defense-in-Depth Protective Strategies,” of the licensee’s fleet CSP states in bullet twelve “The communications voice and data networks (Level 3 type network) provide service for emergency preparedness and security functions required to meet

NUREG-0654 and Section 73.55(j) of 10 CFR requirements. Bi-directional communication with less secure domains is required. Boundary security controls are applied as determined by evaluation performed in accordance with Section 3.1.6 of the Cyber Security Plan.”

Question:

Explain how the bi-directional communications will be secured between communications voice and data networks that will prevent any data transmission to level 3.

Answer:

Level 3 is a security level designation for digital computer and communication systems and networks. Progress Energy has multiple Level 3 type networks which have equivalent protective characteristics. However, based on the functional purpose of the network, different protective equipment may be utilized. In accordance with the Cyber Security Plan and implementation schedule, Level 3 plant computer networks will be deterministically segregated from business computer networks by unidirectional network communications. The communications voice and data networks designated as Level 3 type networks provide service for emergency preparedness and security functions required to meet NUREG-0654 and 10 CFR 73.55(j) requirements. These voice and data networks require bi-directional communication with less secure networks. Boundary security controls and interfaces are applied as determined by an evaluation performed in accordance with Section 3.1.6 of the Cyber Security Plan.

In summary, the Level 3 communications voice and data networks and the Level 3 plant computer network are separate networks based on the functions they support and are not directly connected to each other. The Level 3 plant computer network will be deterministically segregated from the business computer network by unidirectional network in accordance with the Cyber Security Plan. The communications voice and data networks will be segregated from the business computer network by boundary security devices that permit bi-directional communication as determined by an evaluation performed in accordance with Section 3.1.6 of the Cyber Security Plan.