



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

March 10, 2011

Mr. Michael J. Annacone, Vice President
Brunswick Steam Electric Plant
Carolina Power & Light Company
Post Office Box 10429
Southport, North Carolina 28461

Mr. 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

Mr. Eric McCartney, Vice President
H. B. Robinson Steam Electric Plant,
Unit No. 2
Carolina Power & Light Company
3581 West Entrance Road
Hartsville, South Carolina 29550-0790

Mr. Jon A. Franke, Vice President
Crystal River Nuclear Plant (NA2C)
Florida Power & Light Company
ATTN: Supervisor, Licensing & Regulatory
Programs
15760 West Power Line Street
Crystal River, Florida 34428-6708

SUBJECT: BRUNSWICK STEAM ELECTRIC PLANT, UNIT NOS. 1 AND 2; CRYSTAL RIVER UNIT 3 NUCLEAR GENERATING PLANT; H. B. ROBINSON STEAM ELECTRIC PLANT, UNIT NO. 2; AND SHEARON HARRIS NUCLEAR POWER PLANT, UNIT NO. 1 — REQUEST FOR ADDITIONAL INFORMATION REGARDING CYBER SECURITY PLANS BASED ON NUCLEAR ENERGY INSTITUTE 08-09, REVISION 6 (TAC NOS. ME4225, ME4226, ME4227, ME4228, AND ME4229)

Gentlemen:

By letter dated July 8, 2010 (Agencywide Documents Access and Management System, Accession No. ML101950043), Carolina Power & Light Company and Florida Power Corporation (the licensees) resubmitted a request to amend Facility Operating License Nos. DPR-71, DPR-62, DPR-72, NPF 63, and DPR-23 for Brunswick Steam Electric Plant, Unit Nos. 1 and 2; Crystal River Unit 3 Nuclear Generating Plant, Shearon Harris Nuclear Power Plant, Unit No. 1; and H. B. Robinson Steam Electric Plant, Unit No. 2, respectively. Per the proposed license amendments, the licensees requested approval of the above-listed facilities' Cyber Security Plan (CSP), provided a proposed CSP Implementation Schedule, and included proposed revisions to the facilities' operating licenses to incorporate the provisions for implementing and maintaining in effect the provisions of the approved CSP. The licensees' amendment request was based on a generic template developed by the Nuclear Energy Institute in concert with the industry.

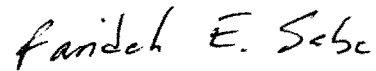
The Nuclear Regulatory Commission (NRC) staff reviewed the licensee's CSP and the proposed CSP Implementation Schedule and determined that additional information is required to perform its technical review. Please see the following requests for additional information (RAIs). These RAIs were reviewed in accordance with the guidance provided in Title 10 of the *Code of Federal Regulations*, Section 2.390, and the NRC staff has determined that no security-related or proprietary information is contained therein.

M. Annacone, et al.

- 2 -

In order for the NRC staff to complete its review in a timely manner, please provide your response within 30 days from the date of this letter. If you have any questions, please contact me at 301-415-1447 or farideh.saba@nrc.gov.

Sincerely,

A handwritten signature in black ink that reads "Farideh E. Saba". The signature is written in a cursive style with a clear, legible font.

Farideh Saba, Senior Project Manager
Plant Licensing Branch II-2
Division of Operating Reactor Licensing
Office of Nuclear Reactor Regulation

Docket Nos. 50-325, 50-324, 50-302,
50-261, and 50-400

Enclosure: RAI

cc w/encl: Distribution via Listserv

REQUEST FOR ADDITIONAL INFORMATION (RAI)

REGARDING CYBER SECURITY PLAN

BRUNSWICK STEAM ELECTRIC PLANT, UNIT NOS. 1 AND 2

CRYSTAL RIVER UNIT 3 NUCLEAR GENERATING PLANT

H. B. ROBINSON STEAM ELECTRIC PLANT, UNIT NO. 2

SHEARON HARRIS NUCLEAR POWER PLANT, UNIT NO. 1

DOCKET NOS. 50-325, 50-260, AND 50-324

DOCKET NO. 50-302

DOCKET NO. 50-400

DOCKET NO. 50-4261

RAI 1: Records Retention

Title 10 of the *Code of Federal Regulations* (10 CFR) 73.54(c)(2) requires licensees to design a cyber security program to ensure the capability to detect, respond to, and recover from cyber attacks. Furthermore, 10 CFR 73.54(e)(2)(i) requires licensees to maintain a cyber security plan that describes how the licensee will maintain the capability for timely detection and response to cyber attacks. The ability for a licensee to detect and respond to cyber attacks requires accurate and complete records and is further supported by 10 CFR 73.54(h), which states that the licensee shall retain all records and supporting technical documentation required to satisfy the requirements of 10 CFR Section 73.54 as a record until the Nuclear Regulatory Commission (NRC) terminates the license for which the records were developed, and shall maintain superseded portions of these records for at least 3 years after the record is superseded, unless otherwise specified by the NRC.

The licensees' Cyber Security Plan (CSP) in Section 4.13 states that Critical Digital Asset (CDA) audit records and audit data (e.g., operating system logs, network device logs) are retained for a period of time that is less than what is required by 10 CFR 73.54(h).

Explain the deviation from the 10 CFR 73.54(h) requirement to retain records and supporting technical documentation until the NRC terminates the license (or to maintain superseded portions of these records for at least 3 years) and how that meets the requirements of 10 CFR 73.54.

RAI 2: Implementation Schedule

The regulation at 10 CFR 73.54, "Protection of digital computer and communication systems and networks," requires licensees to submit a CSP that satisfies the requirements of this section

Enclosure

for NRC review and approval. Furthermore, each submittal must include a proposed implementation schedule and the implementation of the licensees' cyber security program must be consistent with the approved schedule. Paragraph (a) of 10 CFR 73.54 requires licensees to provide high assurance that digital computer and communication systems and networks are adequately protected against cyber attacks, up to and including the design basis threat.

The completion of several key intermediate milestones (Items (a) through (g) below) would demonstrate progress toward meeting the requirements of 10 CFR 73.54. The NRC staff's expectation is that the key intermediate milestones will be completed in a timely manner, but no later than December 31, 2012. The key CSP implementation milestones are as follows:

- (a) Establish, train and qualify Cyber Security Assessment Team, as described in Section 3.1.2, "Cyber Security Assessment Team," of the CSP.
- (b) Identify Critical Systems and CDAs, as described in Section 3.1.3, "Identification of Critical Digital Assets," of the CSP.
- (c) Implement cyber security defense-in-depth architecture by installation of [deterministic one-way] devices, as described in Section 4.3, "Defense-In-Depth Protective Strategies" of the CSP.
- (d) Implement the management, operational and technical cyber security controls that address attacks promulgated by use of portable media, portable devices, and portable equipment as described in Appendix D Section 1.19 "Access Control for Portable and Mobile Devices," of Nuclear Energy Institute (NEI) 08-09, Revision 6.
- (e) Implement observation and identification of obvious cyber related tampering to existing insider mitigation rounds as described in Appendix E Section 4.3, "Personnel Performing Maintenance and Testing Activities," and Appendix E Section 10.3, "Baseline Configuration" of NEI 08-09, Revision 6.
- (f) Identify, document, and implement cyber security controls to physical security target set CDAs in accordance with Section 3.1.6, "Mitigation of Vulnerabilities and Application of Cyber Security Controls," of the CSP.
- (g) Ongoing monitoring and assessment activities will commence for those target set CDAs whose security controls have been implemented, as described in Section 4.4, "Ongoing Monitoring and Assessment," of the CSP
- (h) Full implementation of the CSP for all safety, security, and emergency preparedness functions.

Provide a revised CSP implementation schedule that identifies the appropriate milestones, completion dates, supporting rationale, and level of detail to allow the NRC to evaluate the licensee's proposed schedule and associated milestone dates which include the final completion date. It is the NRC's intention to develop a license condition incorporating your revised CSP implementation schedule containing the key milestone dates.

RAI 3: Scope of Systems

Paragraph (a) of 10 CFR 73.54 requires licensees to provide high assurance that digital computer and communication systems and networks are adequately protected against cyber attacks, up to and including the design basis threat as described in 10 CFR 73.1. In addition, 10 CFR 73.54(a)(1) states that licensees shall protect digital computer and communication systems and networks associated with:

- (i) Safety-related and important-to-safety functions;
- (ii) Security functions;
- (iii) Emergency preparedness functions, including offsite communications; and
- (iv) Support systems and equipment which, if compromised, would adversely impact safety, security, or emergency preparedness functions.

Subsequent to the issuance of the cyber security rule, the NRC stated that 10 CFR 73.54 should be interpreted to include structures, systems, and components (SSCs) in the balance of plant (BOP) that have a nexus to radiological health and safety (Agencywide Documents Access and Management System (ADAMS) Accession No. ML103490344, dated November 19, 2010). The SSCs in the BOP are those that could directly or indirectly affect reactivity of a nuclear power plant and could result in an unplanned reactor shutdown or transient and are therefore, within the scope of important-to-safety functions described in 10 CFR 73.54(a)(1). Furthermore, the NRC issued a letter to NEI dated January 5, 2011 (ADAMS Accession No. ML103550480) that provided licensees with additional guidance on one acceptable approach to comply with the Commission's policy determination.

Explain how the scoping of systems provided by the licensees' CSP for Brunswick Steam Electric Plant Unit, Nos. 1 and 2; Crystal River Unit 3 Nuclear Generating Plant, Shearon Harris Nuclear Power Plant, Unit No. 1; and H.B. Robinson Steam Electric Plant, Unit No. 2 meets the requirements of 10 CFR 73.54 and the additional guidance provided by the NRC.

M. Annacone, et al.

- 2 -

In order for the NRC staff to complete its review in a timely manner, please provide your response within 30 days from the date of this letter. If you have any questions, please contact me at 301-415-1447 or farideh.saba@nrc.gov.

Sincerely,

/RA/

Farideh Saba, Senior Project Manager
Plant Licensing Branch II-2
Division of Operating Reactor Licensing
Office of Nuclear Reactor Regulation

Docket Nos. 50-325, 50-324, 50-302,
50-261, and 50-400

Enclosure: RAI

cc w/encl: Distribution via Listserv

DISTRIBUTION:

PUBLIC
RidsNrrLACSola Resource
RidsRgn2MailCenter Resource
RidsNrrPMShearonHarris
RidsNrrPMCrystalRiver Resource
RidsNrrDorl Resource

LPL2-2 Reading
RidsNrrDorlDpr Resource
RidsAcraAcnw_MailCTR Resource
RidsNrrPMRobinson Resource
RidsNrrPMBrunswick Resource
RidsOgcRp Resource

RidsNrrDorlLp2-2 Resource
C. Erlanger, NSIR
P. Pederson, NSIR
B. Singal, NRR
T. Wengert, NRR

ADAMS Accession No.: ML110620157

OFFICE	LPL2-2/PM	LPL2-2/PM	LPL2-2/LA	LPL2-2/BC	LPL2-2/PM
NAME	FSaba	BMozafari	CSola	DBroaddus	FSaba
DATE	3/8/11	3/8/11	3/8/11	3/9/11	3/10/11

OFFICIAL RECORD COPY