~~SECURITY-RELATED INFORMATION - WITHHOLD UNDER 10 CFR 2.390~~

Progress Energy
411 Fayetteville Street Mall
Raleigh NC 27602

10 CFR 50.4
10 CFR 50.90

Serial: RA-11-011
April 7, 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 INDUSTRY GENERIC REQUEST FOR ADDITIONAL INFORMATION ON THE CAROLINA POWER AND LIGHT COMPANY AND FLORIDA POWER CORPORATION CYBER SECURITY PLAN, REVISION 0

REFERENCES:

1. Progress Energy letter from C. S. Kamilaris to the Nuclear Regulatory Commission Document Control Desk titled, *Request for Approval of the Carolina Power & Light Company and Florida Power Corporation Cyber Security Plan*, dated July 8, 2010, (ML101950043)
2. Progress Energy letter from Garry Miller to the Nuclear Regulatory Commission Document Control Desk titled, *Response to Request for Additional Information on the Carolina Power and Light Company and Florida Power Corporation Cyber Security Plan, Revision 0*, dated February 28, 2011 (ML110670686)
3. Nuclear Regulatory Commission letter from Farideh E. Saba titled, *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)*, dated March 10, 2011, (ML110620157)
4. Nuclear Energy Institute letter from Christopher E. Earls to the Administrative Points of Contact titled *Resolution of Generic issues with Respect to Cyber Security Plans*, dated March 1, 2011

Enclosures 2 and 3 to this letter contain
~~SECURITY-RELATED INFORMATION - WITHHOLD UNDER 10 CFR 2.390~~
Upon removal of Enclosures 2 and 3, this letter is decontrolled.

S001A
NRR

Ladies and Gentlemen:

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 & Light Company and Florida Power Corporation Cyber Security Plan* (Plan) and Implementation Schedule for NRC review and approval in Reference 1. The submittal was supplemented via Reference 2.

An Industry Generic Request for Additional Information (RAI) was received via Reference 3. The generic issues involve cyber security records retention, the Cyber Security Plan implementation schedule, and a clarification on the scope of 10 CFR 73.54 with respect to Balance of Plant (BOP) systems. The Nuclear Energy Institute (NEI) and the Cyber Security Task Force have developed resolutions to these generic issues which have been found acceptable to the Nuclear Regulatory Commission (NRC) staff as discussed in Reference 4.

Enclosure 1 contains the CP&L and FPC response to the Industry Generic RAI. The CP&L and FPC response is consistent with the generic resolutions as documented in Reference 4.

Enclosure 2 contains a revised copy of the *Carolina Power & Light Company and Florida Power Corporation Cyber Security Plan*, Revision 0, which incorporates the changes described in Enclosure 1 and a change described in Reference 2. Changes have been made to the following Plan sections and table:

2.1, Scope and Purpose,
4.3, Defense-In-Depth Protective Strategies,
4.13, Document Control and Records Retention and Handling, and
Table 1 – Deviations From NEI 08-09, Revision 6.

No other changes have been made to the Plan, other than pagination and the addition of accession numbers in Table 1. The enclosed *Carolina Power & Light Company and Florida Power Corporation Cyber Security Plan* replaces, in its entirety, the Plan previously submitted in Reference 1. Enclosure 2 contains security-related information.

Enclosure 3 contains a revised CP&L and FPC Implementation Schedule. This schedule replaces, in its entirety, the Implementation Schedule previously submitted in Reference 1. The implementation milestones listed and associated completion dates are considered to be Regulatory Commitments. These commitments supersede all commitments made in Reference 1. Enclosure 3 contains security-related information.

Enclosure 4 contains a revised mark-up of the Facility Operating License (FOL) pages, for the facilities listed above, which incorporate the License Condition to maintain an NRC approved Cyber Security Plan. The revised FOL mark-ups remove "submitted by letter dated July 8, 2010" from the end of the previously proposed License Condition due to the submittal of multiple Plan supplements. The "Revision 0" identifier is unique to the Plan that will be approved by the NRC.

The changes discussed in this submittal are clarifying or administrative and do not impact the conclusions of the no significant hazards consideration determination previously provided in

Reference 1. However, the description of the change contained in the previously provided no significant hazards consideration has been updated and is provided in Enclosure 5. The enclosed no significant hazards consideration replaces, in its entirety, the no significant hazards consideration previously provided in Reference 1.

CP&L and FPC request that Enclosures 2 and 3, which contain security-related information, be withheld from public disclosure in accordance with 10 CFR 2.390.

This submittal contains regulatory commitments as identified in Enclosure 3. These commitments supersede all commitments previously made in Reference 1.

If you have questions regarding this submittal, please contact Donna Alexander, Interim Manager, Nuclear Regulatory Affairs, at (919) 546-5357.

I declare under the penalty of perjury that the foregoing is true and correct. Executed on April 7, 2011.

Sincerely,

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

DBM

Enclosures:

1. Response to Industry Generic Request for Additional Information on the *Carolina Power & Light Company and Florida Power Corporation Cyber Security Plan*, Revision 0
2. *Carolina Power & Light Company and Florida Power Corporation Cyber Security Plan*, Revision 0 (contains security-related information)
3. Cyber Security Plan Implementation Schedule (contains security-related information)
4. Marked-up Facility Operating License Pages
5. Updated No Significant Hazards Consideration

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

Enclosures 2 and 3 to this letter contain
~~SECURITY-RELATED INFORMATION - WITHHOLD UNDER 10 CFR 2.390~~
Upon removal of Enclosures 2 and 3, this letter is decontrolled.

cc w/o Enclosures 2 and 3:
State of Florida Contact
Chair – North Carolina Utilities Commission
W. L. Cox, III, Section Chief N.C. DENR
S. E. Jenkins, Manager, Infectious and Radioactive Waste Management Section (SC)
A. Gantt, Chief, Bureau of Radiological Health (SC)
Attorney General (SC)

Enclosures 2 and 3 to this letter contain
~~SECURITY-RELATED INFORMATION - WITHHOLD UNDER 10 CFR 2.390~~
Upon removal of Enclosures 2 and 3, this letter is decontrolled.

ENCLOSURE 1

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

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

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.

Response:

Section 4.13, "Document Control and Records Retention and Handling," of the *Carolina Power & Light Company and Florida Power Corporation Cyber Security Plan* (Plan) has been changed consistent with the language provided to the Nuclear Regulatory Commission (NRC) staff by the Nuclear Energy Institute (NEI).[1] This change is a deviation from NEI 08-09, Appendix A, Revision 6, but was found to be acceptable by the NRC staff.[2] The deviation is documented in Table 1, "Deviations from NEI 08-09, Revision 6," of the Plan.

[1] NEI letter from Christopher E. Earls to Richard P. Correia, (NRC), *Clarification of NEI 08-09, Revision 6 Regarding Records Retention*, dated February 28, 2011, (Agencywide Documents Access and Management System (ADAMS) Accession No. ML110600204 & ML110600205)

[2] NRC letter from Richard P. Correia to Christopher E. Earls (NEI), *Cyber Security Plan Generic Request for Additional Information on Records Retention*, dated March 1, 2011, (ML110490337)

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 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.

Response:

A revised *Carolina Power & Light Company and Florida Power Corporation Cyber Security Plan* Implementation Schedule is enclosed with this submittal. The enclosed implementation schedule is consistent with the Cyber Security Plan Implementation Schedule template sent to the NRC staff by NEI.[3] The Cyber Security Plan Implementation Schedule template was found to be acceptable by the NRC staff.[4]

[3] NEI letter from Christopher E. Earls to Richard P. Correia (NRC), *Template for the Cyber Security Plan Implementation Schedule*, dated February 28, 2011, (ML110600211 & ML110600218)
[4] NRC Letter from Richard P. Correia to Christopher E. Earls (NEI), *Template for the Cyber Security Plan Implementation Schedule*, dated March 1, 2011, (ML110070348)

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. ML 103550480) 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.

Answer:

Section 2.1, Scope and Purpose, of the *Carolina Power & Light Company and Florida Power Corporation Cyber Security Plan* (Plan) has been changed to add the following paragraph.

> Within the scope of NRC's cyber security rule at Title 10 of the *Code of Federal Regulations* (10 CFR) 73.54, systems or equipment that perform important to safety functions include structures, systems, and components (SSCs) in the balance of plant (BOP) that could directly or indirectly affect reactivity at a nuclear power plant and could result in an unplanned reactor shutdown or transient. Additionally, these SSCs are under the licensee's control and include electrical distribution equipment out to the first inter-tie with the offsite distribution system.

This change was made in accordance with direction provided to NEI by the NRC.[5] This change is a deviation from NEI 08-09, Appendix A, Revision 6, and is documented in Table 1, "Deviations from NEI 08-09, Revision 6," of the Plan.

[5] NRC letter from Richard P. Correia to Chris Earls (NEI) dated January 5, 2011, (ML103550480)

Enclosure 4

Marked-up Facility Operating License Pages

Enclosure 4

Marked-up Facility Operating License Pages

Carolina Power & Light Company – Brunswick Steam Electric Plant, Unit No. 1

at the end of the first surveillance interval that begins on the date the Surveillance was last performed prior to implementation of Amendment 203.

(a) Effective June 30, 1982, the surveillance requirements listed below need not be completed until July 15, 1982. Upon accomplishment of the surveillances, the provisions of Technical Specification 4.0.2 shall apply.

Specification 4.3.3.1, Table 4.3.3-1, Items 5.a and 5.b

(b) Effective July 1, 1982, through July 8, 1982, Action statement "a" Technical Specification 3.8.1.1 shall read as follows:

ACTION:

a. With either one offsite circuit or one diesel generator of the above required A.C. electrical power sources inoperable, demonstrate the OPERABILITY of the remaining A.C. sources by performing Surveillance Requirements 4.8.1.1.1.a and 4.8.1.1.2.a.4 within two hours and at least once per 12 hours thereafter; restore at least two offsite circuits and four diesel generators to OPERABLE status within 7 days or be in at least HOT SHUTDOWN within the next 12 hours and in COLD SHUTDOWN within the following 24 hours.

physical security, training and qualification, and safeguards contingency

, and cyber security

(3) Deleted by Amendment No. 206.

D. The licensee shall fully implement and maintain in effect all provisions of the Commission-approved physical security, training and qualification, ~~and~~ safeguards contingency plans, including amendments made pursuant to provisions of the Miscellaneous Amendments and Search Requirements revisions to 10 CFR 73.55 (51 FR 27817 and 27822) and to the authority of 10 CFR 50.90 and 10 CFR 50.54(p). The plans, which contain Safeguards Information protected under 10 CFR 73.21 are entitled: "Physical Security Plan, Revision 2," and "Safeguards Contingency Plan, Revision 2," submitted by letter dated May 17, 2006, and "Guard Training and Qualification Plan, Revision 0," submitted by letter dated September 30, 2004.

E. This license is subject to the following additional conditions for the protection of the environment:

a. Deleted per Amendment 54, 3-11-83

b. Deleted per Amendment 54, 3-11-83

c. The licensee shall comply with the effluent limitations contained in National Pollutant Discharge Elimination System Permit No. NC0007064

The cyber security plan, which contains security-related information withheld from public disclosure under 10 CFR 2.390, is entitled: "Carolina Power & Light Company and Florida Power Corporation Cyber Security Plan, Revision 0."

Enclosure 4

Marked-up Facility Operating License Pages

Carolina Power & Light Company – Brunswick Steam Electric Plant, Unit No. 2

physical security, training and qualification, and safeguards contingency

(4) Equalizer Valve Restriction

The valves in the equalizer piping between the recirculation loops shall be closed at all times during reactor operation, except for one bypass valve which is left open to prevent pressure build-up due to ambient and conduction heating of the water between the equalizer valves.

(5) Deleted by Amendment No. 233.

, and cyber security

(6) The licensee shall fully implement and maintain in effect all provisions of the Commission-approved physical security, training and qualification, and safeguards contingency plans, including amendments made pursuant to provisions of the Miscellaneous Amendments and Search Requirements revisions to 10 CFR 73.55 (51 FR 27817 and 27822) and to the authority of 10 CFR 50.90 and 10 CFR 50.54(p). The plans, which contain Safeguards Information protected under 10 CFR 73.21, are entitled: "Physical Security Plan, Revision 2," and "Safeguards Contingency Plan, Revision 2," submitted by letter dated May 17, 2006, and "Guard Training and Qualification Plan, Revision 0," submitted by letter dated September 30, 2004.

D. This license is subject to the following additional conditions for the protection of the environment:

a. Deleted per Amendment 79, 3-11-83

b. Deleted per Amendment 79, 3-11-83

c. Deleted per Amendment 79, 3-11-83

d. The licensee shall comply with the effluent limitations contained in National Pollutant Discharge Elimination System Permit No. NC0007064 issued pursuant to Section 402 of the Federal Water Pollution Control Act, as amended.

E. This license is effective as of the date of issuance and shall expire at midnight on December 27, 2034.

F. Deleted per Amendment No. 98 dated 5-25-84.

G. Deleted per Amendment No. 98 dated 5-25-84.

H. Deleted by Amendment No. 236.

I. Power Uprate License Amendment Implementation

The licensee shall complete the following actions as a condition of the approval of the power uprate license amendment (Amendment No. 214):

The cyber security plan, which contains security-related information withheld from public disclosure under 10 CFR 2.390, is entitled: "Carolina Power & Light Company and Florida Power Corporation Cyber Security Plan, Revision 0."

Enclosure 4

Marked-up Facility Operating License Pages

Carolina Power & Light Company – Shearon Harris Nuclear Power Plant, Unit No. 1

, and cyber security

physical security, training and qualification, and safeguards contingency

E. Physical Security (Section 13.6.2.10)

The licensee shall fully implement and maintain in effect all provisions of the Commission-approved physical security, training and qualification, ~~and~~ safeguards contingency plans including amendments made pursuant to provisions of the Miscellaneous Amendments and Search Requirements revisions to 10 CFR 73.55 (51 FR 27817 and 27822) and the authority of 10 CFR 50.90 and 10 CFR 50.54(p). The plans, which contain Safeguards Information protected under 10 CFR 73.21, are entitled: "Guard Training and Qualification Plan" submitted by letter dated October 19, 2004, "Physical Security Plan" and "Safeguards Contingency Plan" submitted by letter dated October 19, 2004 as supplemented by letter dated May 16, 2006.

F. Fire Protection Program

Carolina Power & Light Company shall implement and maintain in effect all provisions of the approved fire protection program that comply with 10 CFR 50.48(a) and 10 CFR 50.48(c), as specified in the revised license amendment request dated October 9, 2009, supplemented by letters dated February 4, 2010, and April 5, 2010, and approved in the associated safety evaluation dated June 28, 2010. Except where NRC approval for changes or deviations is required by 10 CFR 50.48(c) and NFPA 805, and provided no other regulation, technical specification, license condition or requirement would require prior NRC approval, the licensee may make changes to the fire protection program without prior approval of the Commission if those changes satisfy the provisions set forth in 10 CFR 50.48(a) and 10 CFR 50.48(c), the change does not require a change to a technical specification or a license condition, and the criteria listed below are satisfied.

(1) Risk-Informed Changes that May Be Made Without Prior NRC Approval

A risk assessment of the change must demonstrate that the acceptance criteria below are met. The risk assessment approach, methods, and data shall be acceptable to the NRC and shall be appropriate for the nature and scope of the change being evaluated; be based on the as-built, as-operated and maintained plant; and reflect the operating experience at the plant. Acceptable methods to assess the risk of the proposed change may include methods that have been used in the peer-reviewed Fire PRA model, methods that have been approved by the NRC via a plant-specific license amendment or through NRC approval of generic methods specifically for use in NFPA 805 risk assessments, or methods that have been demonstrated to bound the risk impact.

(a) Prior NRC review and approval is not required for changes that clearly result in a decrease in risk. The proposed change must also be consistent with the defense-in-depth philosophy and must maintain sufficient safety margins. The change may be implemented following completion of the plant change evaluation.

The cyber security plan, which contains security-related information withheld from public disclosure under 10 CFR 2.390, is entitled: "Carolina Power & Light Company and Florida Power Corporation Cyber Security Plan, Revision 0."

Enclosure 4

Marked-up Facility Operating License Pages

Carolina Power & Light Company – H. B. Robinson Steam Electric Plant, Unit No. 2

C. Reports

Carolina Power & Light Company shall make certain reports in accordance with the requirements of the Technical Specifications.

D. Records

Carolina Power & Light Company shall keep facility operating records in accordance with the requirements of the Technical Specifications.

E. Fire Protection Program

Carolina Power & Company shall implement and maintain in effect all provisions of the approved Fire Protection Program as described in the Updated Final Safety Analysis Report for the facility and as approved in the Fire Protection Safety Evaluation Report dated February 28, 1978, and supplements thereto. Carolina Power & Light Company may make changes to the approved Fire Protection Program without prior approval of the Commission only if those changes would not adversely affect the ability to achieve and maintain safe shutdown in the event of a fire.

F. Physical Protection

, and cyber security plans,

The licensee shall fully implement and maintain in effect all provisions of the Commission-approved physical security, training and qualification, and safeguards contingency ~~plans~~ including amendments made pursuant to provisions of the Miscellaneous Amendments and Search Requirements revisions to 10 CFR 73.55 (51 FR 27817 and 27822) and the authority of 10 CFR 50.90 and 10 CFR 50.54(p). The combined set of plans, which contains Safeguards Information protected under 10 CFR 73.21, is entitled: "H. B. Robinson Steam Electric Plant Security, Training and Qualification, and Safeguards Contingency Plan, Revision 0" submitted by letter dated October 1, 2004, as supplemented by letter dated October 20, 2004.

G. The following programs shall be implemented and maintained by the licensee:

(1) DELETED

The cyber security plan, which contains security-related information withheld from public disclosure under 10 CFR 2.390, is entitled: "Carolina Power & Light Company and Florida Power Corporation Cyber Security Plan, Revision 0."

physical security, training and qualification, and safeguards contingency

Enclosure 4

Marked-up Facility Operating License Pages

Florida Power Corporation – Crystal River Unit 3

- 5d-

2.D Mitigation Strategy License Condition

The licensee shall fully implement and maintain in effect all provisions of the Commission-approved physical security, training and qualification, ~~and~~ safeguards contingency ~~plans~~, and cyber security plans, including amendments made pursuant to provisions of the Miscellaneous Amendments and Search Requirements revisions to 10 CFR 73.55 (51 FR 27817 and 27822) and to the authority of 10 CFR 50.90 and 10 CFR 50.54(p). The physical security, training and qualification, and safeguards contingency plans, which contain Safeguards Information protected under 10 CFR 73.21, are entitled: "Physical Security Plan, Revision 5," and "Safeguards Contingency Plan, Revision 4," submitted by letter dated May 16, 2006, and "Guard Training and Qualification Plan, Revision 0," submitted by letter dated September 30, 2004, as supplemented by letters dated October 20, 2004, and September 29, 2005. The cyber security plan, which contains security-related information withheld from public disclosure under 10 CFR 2.390, is entitled: "Carolina Power & Light Company and Florida Power Corporation Cyber Security Plan, Revision 0."

Enclosure 5

Updated No Significant Hazards Consideration

4.0 REGULATORY EVALUATION

4.1 APPLICABLE REGULATORY REQUIREMENTS / CRITERIA

This LAR is submitted pursuant to 10 CFR 73.54 which requires licensees currently licensed to operate a nuclear power plant under 10 CFR Part 50 to submit a Cyber Security Plan as specified in 10 CFR 50.4 and 10 CFR 50.90.

4.2 NO SIGNIFICANT HAZARDS CONSIDERATION

Carolina Power & Light Company (CP&L) and Florida Power Corporation (FPC) have evaluated the proposed changes using the criteria in 10 CFR 50.92 and have determined that the proposed changes do not involve a significant hazards consideration. An analysis of the issue of no significant hazards consideration is presented below.

The proposed change incorporates a new requirement into the FOLs to implement and maintain a Cyber Security Plan. This new requirement is being included as part of an existing FOL condition that requires the implementation and maintenance of physical security, training and qualification, and safeguards contingency plans. The Cyber Security Plan describes how the requirements of 10 CFR 73.54 will be implemented in order to protect the health and safety of the public from radiological sabotage as a result of a cyber attack threat described in 10 CFR 73.1. The plan conforms to the template provided in NEI 08-09, Revision 6, with three deviations regarding records retention, balance of plant regulatory jurisdiction, and the definition of Cyber Attack, and provides a description of how the requirements of 10 CFR 73.54 will be implemented at Brunswick Steam Electric Plant (BSEP), Unit Nos. 1 and 2; Crystal River Unit 3 (CR-3); Shearon Harris Nuclear Power Plant, Unit No. 1 (HNP); and H. B. Robinson Steam Electric Plant (HBRSEP), Unit No. 2. The Cyber Security Plan establishes the licensing basis for the Cyber Security Program for BSEP, Unit Nos. 1 and 2; CR-3; HNP; and HBRSEP, Unit No. 2. The Cyber Security Plan establishes how to achieve high assurance that nuclear power plant digital computer and communication systems and networks associated with the following are adequately protected against cyber attacks, up to and including the design basis threat:

1. Safety-related and important-to-safety functions,
2. Security functions,
3. Emergency preparedness functions including offsite communications, and
4. Support systems and equipment which if compromised, would adversely impact safety, security, or emergency preparedness functions.

Criterion 1: The proposed change does not involve a significant increase in the probability or consequences of an accident previously evaluated.

The proposed change incorporates a new requirement, in the FOL, to implement and maintain a Cyber Security Plan as part of the facility's overall program for physical protection. The Cyber Security Plan itself does not require any plant modifications. Rather, the Cyber Security Plan describes how the requirements of 10 CFR 73.54 are implemented in order to identify, evaluate, and mitigate cyber attacks up to and including the design basis threat, thereby achieving high assurance that the facility's digital computer and communications systems and networks are protected from cyber attacks.

The proposed change requiring the implementation and maintenance of a Cyber Security Plan does not alter the plant configuration, require new plant equipment to be installed, alter accident analysis assumptions, add any accident initiators, or affect the function of plant systems or the manner in which systems are operated, maintained, modified, tested, or inspected; therefore, the inclusion of the Cyber Security Plan as a part of the facility's other physical protection programs specified in the FOL has no impact on the probability or consequences of an accident previously evaluated.

Criterion 2: The proposed change does not create the possibility of a new or different kind of accident from any accident previously evaluated.

The proposed change incorporates a new requirement, in the FOL, to implement and maintain a Cyber Security Plan as part of the facility's overall program for physical protection. The creation of the possibility of a new or different kind of accident requires creating one or more new accident precursors. New accident precursors may be created by modifications of the plant's configuration, including changes in the allowable modes of operation. The Cyber Security Plan itself does not require any plant modifications, nor does the Cyber Security Plan affect the control parameters governing unit operation or the response of plant equipment to a transient condition. Because the proposed change does not change or introduce any new equipment, modes of system operation, or failure mechanisms, no new accident precursors are created. Therefore, the proposed change does not create the possibility of a new or different kind of accident from any accident previously evaluated.

Criterion 3: The proposed change does not involve a significant reduction in a margin of safety.

The proposed change incorporates a new requirement, in the FOL, to implement and maintain a Cyber Security Plan as part of the facility's overall program for physical protection. Plant safety margins are established through Limiting Conditions for Operation, Limiting Safety System Settings and Safety Limits specified in the Technical Specifications. Because the Cyber Security Plan does not require any plant modifications and does not alter the operation of plant equipment, the proposed change does not change established safety margins. Therefore, the proposed change does not involve a significant reduction in a margin of safety.

4.3 CONCLUSIONS

Based on the above, CP&L and FPC conclude that the proposed change presents no significant hazards consideration under the standards set forth in 10 CFR 50.92(c), and accordingly, a finding of no significant hazards consideration is justified.