



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

July 29, 2011

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

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

Robert J. Duncan II, 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. William Jefferson, 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: BRUNSWICK STEAM ELECTRIC PLANT, UNITS 1 AND 2, H. B. ROBINSON STEAM ELECTRIC PLANT, UNIT NO. 2, SHEARON HARRIS NUCLEAR POWER PLANT, UNIT 1, AND CRYSTAL RIVER UNIT 3 NUCLEAR GENERATING PLANT — ISSUANCE OF LICENSE AMENDMENTS REGARDING APPROVAL OF CYBER SECURITY PLAN (TAC NOS. ME4225, ME4226, ME4227, ME4228, AND ME4229)

Gentlemen:

By letter dated July 8, 2010, as supplemented by letters dated September 23 and November 30, 2010; February 28 and April 7, 2011, Carolina Power & Light Company and Florida Power Corporation (the licensees) submitted a request to amend Renewed Facility Operating License Nos. DPR-71, DPR-62, DPR-23, and NPF 63; and Facility Operating License No. DPR-72 for Brunswick Steam Electric Plant (BSEP) Units 1 and 2, H.B. Robinson Steam Electric Plant, Unit No. 2 (RSEP-2), Shearon Harris Nuclear Power Plant, Unit 1 (HNP-1), and Crystal River Unit 3 Nuclear Generating Plant (CR 3), respectively.

The licensees' submittal was in accordance with the requirements of Title 10 of the *Code of Federal Regulations* (10 CFR) 73.54 and generally consistent with the template contained in Nuclear Energy Institute (NEI) 08-09, Revision 6, "Cyber Security Plan for Nuclear Power Reactors," dated April 2010. In a letter to NEI dated May 5, 2010, the U.S. Nuclear Regulatory Commission (NRC) staff concluded that submission of a CSP using the template provided in NEI 08-09, Revision 6 would be acceptable for use by licensees with the exception of the definition of "cyber attack." The NRC staff subsequently reviewed and approved by letter dated June 7, 2010, a revised definition for "cyber attack" for use in the licensees' submittals that were based on NEI 08-09, Revision 6.

The NRC staff has completed its review of the licensees' submittals and found that the licensees' CSPs meet the requirements of 10 CFR 73.54 and upon successful implementation

M. Annacone, et al.

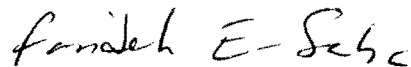
- 2 -

of this program, operation of the BSEP, Units 1 and 2, RSEP- 2, HNP-1, and CR-3 will not be inimical to the common defence and security.

The amendments approve the licensees' proposed cyber security plans and associated implementation schedule; revise Renewed Facility Operating License Nos. DPR-71, DPR-62, DPR-23; NPF 63, for BSEP, Unit Nos. 1 and 2, RBSEP-2, and HNP-1, respectively, and Facility Operating License No. DPR-72 for CR-3; and add a license condition to require the licensees to fully implement and maintain in effect all provisions of the NRC-approved Cyber Security Plan.

A copy of the NRC staff related safety evaluation (SE) is enclosed. The enclosed SE was reviewed in accordance with the guidance provided in 10 CFR 2.390, and the NRC Staff has determined that no security-related or proprietary information is contained therein. The Notice of Issuance will be included in the Commission's next biweekly *Federal Register* notice. If you have any questions, please contact me at 301 415-1447 or Farideh.Saba@nrc.gov.

Sincerely,



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

Enclosures:

1. Amendment No. 258 to DPR-71
2. Amendment No. 286 to DPR-62
3. Amendment No. 226 to DPR-23
4. Amendment No. 136 to NPF-63
5. Amendment No. 238 to DPR-72
6. Safety Evaluation

cc: Distribution via Listserv



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

CAROLINA POWER & LIGHT COMPANY

DOCKET NO. 50-325

BRUNSWICK STEAM ELECTRIC PLANT, UNIT 1

AMENDMENT TO RENEWED FACILITY OPERATING LICENSE

Amendment No. 258
Renewed License No. DPR-71

1. The Nuclear Regulatory Commission (the Commission) has found that:
 - A. The application for amendment filed by Carolina Power & Light Company (the licensee), dated July 8, 2010, as supplemented by letters dated September 23 and November 30, 2010; February 28 and April 7, 2011, complies with the standards and requirements of the Atomic Energy Act of 1954, as amended (the Act), and the Commission's rules and regulations set forth in Title 10 of the *Code of Federal Regulations* (10 CFR) Chapter I;
 - B. The facility will operate in conformity with the application, the provisions of the Act, and the rules and regulations of the Commission;
 - C. There is reasonable assurance (i) that the activities authorized by this amendment can be conducted without endangering the health and safety of the public, and (ii) that such activities will be conducted in compliance with the Commission's regulations;
 - D. The issuance of this amendment will not be inimical to the common defense and security or to the health and safety of the public; and
 - E. The issuance of this amendment is in accordance with 10 CFR Part 51 of the Commission's regulations and all applicable requirements have been satisfied.

2. Accordingly, the license is amended as indicated in the attachment to this license amendment, and paragraph 2.C.(2) of Renewed Facility Operating License No. DPR-71 is hereby amended to read as follows:

(2) Technical Specifications

The Technical Specifications contained in Appendices A and B, as revised through Amendment No. 258, are hereby incorporated in the license. Carolina Power & Light Company shall operate the facility in accordance with the Technical Specifications.

3. In addition, Paragraph 2.D of Renewed Facility Operating License No. DPR-71 is revised to add the following language:

The licensee shall fully implement and maintain in effect all provisions of the Commission-approved cyber security plan (CSP), including changes made pursuant to the authority of 10 CFR 50.90 and 10 CFR 50.54(p). The licensee's CSP was approved by License Amendment No. 258.

4. This license amendment is effective as of the date of its issuance. The implementation of the CSP, including the key intermediate milestone dates and the full implementation date, shall be in accordance with the implementation schedule submitted by the licensee on April 7, 2011, and approved by the NRC staff with this license amendment. All subsequent changes to the NRC-approved CSP implementation schedule will require prior NRC approval pursuant to 10 CFR 50.90.

FOR THE NUCLEAR REGULATORY COMMISSION



Douglas A. Broaddus, Chief
Plant Licensing Branch II-2
Division of Operating Reactor Licensing
Office of Nuclear Reactor Regulation

Attachment:
Changes to Renewed
License No. DPR-71

Date of Issuance: July 29, 2011

ATTACHMENT TO LICENSE AMENDMENT NO. 258

RENEWED FACILITY OPERATING LICENSE NO. DPR-71

DOCKET NO. 50-325

Replace the following pages of Renewed Operating License DPR-71 with the attached revised pages. The revised pages are identified by amendment number and contain marginal lines indicating the areas of change.

Remove Pages

4

Insert Pages

4

4a

(2) Technical Specifications

The Technical Specifications contained in Appendix A, as revised through Amendment No. 258, are hereby incorporated in the license. Carolina Power & Light Company shall operate the facility in accordance with the Technical Specifications.

For Surveillance Requirements (SRs) that are new in Amendment 203 to Renewed Facility Operating License DPR-71, the first performance is due at the end of the first surveillance interval that begins at implementation of Amendment 203. For SRs that existed prior to Amendment 203, including SRs with modified acceptance criteria and SRs whose frequency of performance is being extended, the first performance is due 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" of 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.A. 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.

- (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.

The licensee shall fully implement and maintain in effect all provisions of the Commission-approved cyber security plan (CSP), including changes made pursuant to the authority of 10 CFR 50.90 and 10 CFR 50.54(p). The licensee's CSP was approved by License Amendment No. 258.



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

CAROLINA POWER & LIGHT COMPANY

DOCKET NO. 50-324

BRUNSWICK STEAM ELECTRIC PLANT, UNIT 2

AMENDMENT TO RENEWED FACILITY OPERATING LICENSE

Amendment No. 286
Renewed License No. DPR-62

1. The Nuclear Regulatory Commission (the Commission) has found that:
 - A. The application for amendment filed by Carolina Power & Light Company (the licensee), dated July 8, 2011, as supplemented by letters dated September 23 and November 30, 2010; February 28 and April 7, 2011, complies with the standards and requirements of the Atomic Energy Act of 1954, as amended (the Act) and the Commission's rules and regulations set forth in Title 10 of the *Code of Federal Regulations* (10 CFR) Chapter I;
 - B. The facility will operate in conformity with the application, the provisions of the Act, and the rules and regulations of the Commission;
 - C. There is reasonable assurance (i) that the activities authorized by this amendment can be conducted without endangering the health and safety of the public, and (ii) that such activities will be conducted in compliance with the Commission's regulations;
 - D. The issuance of this amendment will not be inimical to the common defense and security or to the health and safety of the public; and
 - E. The issuance of this amendment is in accordance with 10 CFR Part 51 of the Commission's regulations and all applicable requirements have been satisfied.

2. Accordingly, the license is amended as indicated in the attachment to this license amendment, and paragraph 2.C.(2) of Renewed Facility Operating License No. DPR-62 is hereby amended to read as follows:

(2) Technical Specifications

The Technical Specifications contained in Appendices A and B, as revised through Amendment No. 286, are hereby incorporated in the license. The Carolina Power & Light Company shall operate the facility in accordance with the Technical Specifications.

3. In addition, Paragraph 2.C.(6) of Facility Operating License No. DPR-62 is revised to add the following language:

The licensee shall fully implement and maintain in effect all provisions of the Commission-approved cyber security plan (CSP), including changes made pursuant to the authority of 10 CFR 50.90 and 10 CFR 50.54(p). The licensee's CSP was approved by License Amendment No. 286.

4. This license amendment is effective as of the date of its issuance. The implementation of the CSP, including the key intermediate milestone dates and the full implementation date, shall be in accordance with the implementation schedule submitted by the licensee on April 7, 2011, and approved by the NRC staff with this license amendment. All subsequent changes to the NRC-approved CSP implementation schedule will require prior NRC approval pursuant to 10 CFR 50.90.

FOR THE NUCLEAR REGULATORY COMMISSION



Douglas A. Broaddus, Chief
Plant Licensing Branch II-2
Division of Operating Reactor Licensing
Office of Nuclear Reactor Regulation

Attachment:
Changes to Renewed
License No. DPR-62

Date of Issuance: July 29, 2011

ATTACHMENT TO LICENSE AMENDMENT NO. 286

RENEWED FACILITY OPERATING LICENSE NO. DPR-62

DOCKET NO. 50-324

Replace the following pages of Renewed Operating License DPR-62 with the attached revised pages. The revised pages are identified by amendment number and contain marginal lines indicating the areas of change.

Remove Pages

3
5

Insert Pages

3
5
5a

as sealed neutron sources for reactor startup, sealed sources for reactor instrumentation and radiation monitoring equipment calibration, and as fission detectors in amounts as required;

(4) Pursuant to the Act and 10 CFR Parts 30, 40 and 70, to receive, possess and use in amounts as required any byproduct, source, and special nuclear materials without restriction to chemical or physical form, for sample analysis or instrument calibration or associated with radioactive apparatus or components;

(5) Pursuant to the Act and 10 CFR Parts 30 and 70 to possess, but not separate, such byproduct and special nuclear materials as may be produced by the operation of Brunswick Steam Electric Plant, Unit Nos. 1 and 2, and H. B. Robinson Steam Electric Plant, Unit No. 2;

(6) Carolina Power & Light Company shall implement and maintain in effect all provisions of the approved fire protection program as described in the Final Safety Analysis Report for the facility and as approved in the Safety Evaluation Report dated November 22, 1977, as supplemented April 1979, June 11, 1980, December 30, 1986, December 6, 1989, July 28, 1993, and February 10, 1994 respectively, subject to the following provision:

The licensee 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.

C. This renewed license shall be deemed to contain and is subject to the conditions specified in the following Commission regulations in 10 CFR Chapter I: Part 20, Section 30.34 of Part 30, Section 40.41 of Part 40, Sections 50.54 and 50.59 of Part 50, and Section 70.32 of Part 70; is subject to all applicable provisions of the Act and to the rules, regulations, and orders of the Commission now or hereafter in effect; and is subject to the additional conditions specified or incorporated below:

(1) Maximum Power Level

The licensee is authorized to operate the facility at steady state reactor core power levels not in excess of 2923 megawatts (thermal).

(2) Technical Specifications

The Technical Specifications contained in Appendix A, as revised through Amendment No. 286, are hereby incorporated in the license. Carolina Power & Light Company shall operate the facility in accordance with the Technical Specifications.

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.

(3) Deleted by Amendment No. 236.

(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.

(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.

The licensee shall fully implement and maintain in effect all provisions of the Commission-approved cyber security plan (CSP), including changes made pursuant to the authority of 10 CFR 50.90 and 10 CFR 50.54(p). The licensee's CSP was approved by License Amendment No. 286.

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.

- 5a -

- 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.

Renewed License No. DPR-62
Amendment No. 286



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

CAROLINA POWER & LIGHT COMPANY

DOCKET NO. 50-261

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

AMENDMENT TO RENEWED FACILITY OPERATING LICENSE

Amendment No. 226
Renewed License No. DPR-23

1. The Nuclear Regulatory Commission (the Commission) has found that:
 - A. The application for amendment by Carolina Power & Light Company (the licensee), dated July 8, 2011, as supplemented by letters dated September 23 and November 30, 2010; February 28 and April 7, 2011, complies with the standards and requirements of the Atomic Energy Act of 1954, as amended (the Act), and the Commission's rules and regulations set forth in Title 10 of the *Code of Federal Regulations* (10 CFR) Chapter I;
 - B. The facility will operate in conformity with the application, the provisions of the Act, and the rules and regulations of the Commission;
 - C. There is reasonable assurance (i) that the activities authorized by this amendment can be conducted without endangering the health and safety of the public, and (ii) that such activities will be conducted in compliance with the Commission's regulations;
 - D. The issuance of this amendment will not be inimical to the common defense and security or to the health and safety of the public; and
 - E. The issuance of this amendment is in accordance with 10 CFR Part 51 of the Commission's regulations and all applicable requirements have been satisfied.

2. Accordingly, the license is amended as indicated in the attachment to this license amendment, and paragraph 3.B. of Renewed Facility Operating License No. DPR-23 is hereby amended to read as follows:

B. Technical Specifications

The Technical Specifications contained in Appendix A, as revised through Amendment No. 226 are hereby incorporated in the license.

3. In addition, Paragraph 3.F of Renewed Facility Operating License No. DPR-23 is revised to add the following language:

The licensee shall fully implement and maintain in effect all provisions of the Commission-approved cyber security plan (CSP), including changes made pursuant to the authority of 10 CFR 50.90 and 10 CFR 50.54(p). The licensee's CSP was approved by License Amendment No. 226 .

4. This license amendment is effective as of the date of its issuance. The implementation of the CSP, including the key intermediate milestone dates and the full implementation date, shall be in accordance with the implementation schedule submitted by the licensee on April 7, 2011, and approved by the NRC staff with this license amendment. All subsequent changes to the NRC-approved CSP implementation schedule will require prior NRC approval pursuant to 10 CFR 50.90.

FOR THE NUCLEAR REGULATORY COMMISSION



Douglas A. Broaddus, Chief
Plant Licensing Branch II-2
Division of Operating Reactor Licensing
Office of Nuclear Reactor Regulation

Attachment:
Changes to Renewed
License No. DPR-23

Date of Issuance: July 29, 2011

ATTACHMENT TO LICENSE AMENDMENT NO. 226

RENEWED FACILITY OPERATING LICENSE NO. DPR-23

DOCKET NO. 50-261

Replace the following pages of the Renewed Facility Operating License No. DPR-23 with the attached revised pages. The revised pages are identified by amendment number and contain marginal lines indicating the areas of change.

Remove Pages

3
4

Insert Pages

3
4

neutron sources for reactor startup, sealed sources for reactor instrumentation and radiation monitoring equipment calibration, and as fission detectors in amounts as required;

- D. Pursuant to the Act and 10 CFR Parts 30, 40 and 70, to receive, possess, and use in amounts as required any byproduct, source, or special nuclear material without restriction to chemical or physical form for sample analysis or instrument and equipment calibration or associated with radioactive apparatus or components;
 - E. Pursuant to the Act and 10 CFR Parts 30 and 70, to possess, but not separate, such byproduct and special nuclear materials as may be produced by operation of the facility.
3. This renewed license shall be deemed to contain and is subject to the conditions specified in the following Commission regulations: 10 CFR Part 20, Section 30.34 of 10 CFR Part 30, Section 40.41 of 10 CFR Part 40, Section 50.54 and 50.59 of 10 CFR Part 50, and Section 70.32 of 10 CFR Part 70; and is subject to all applicable provisions of the Act and to the rules, regulations, and orders of the Commission now or hereafter in effect; and is subject to the additional conditions specified or incorporated below:
- A. Maximum Power Level

The licensee is authorized to operate the facility at a steady state reactor core power level not in excess of 2339 megawatts thermal.
 - B. Technical Specifications

The Technical Specifications contained in Appendix A, as revised through Amendment No. 226 are hereby incorporated in the license.

The licensee shall operate the facility in accordance with the Technical Specifications.
 - (1) For Surveillance Requirements (SRs) that are new in Amendment 176 to Final Operating License DPR-23, the first performance is due at the end of the first surveillance interval that begins at implementation of Amendment 176. For SRs that existed prior to Amendment 176, including SRs with modified acceptance criteria and SRs whose frequency of performance is being extended, the first performance is due at the end of the first surveillance interval that begins on the date the Surveillance was last performed prior to implementation of Amendment 176.

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

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.

The licensee shall fully implement and maintain in effect all provisions of the Commission-approved cyber security plan (CSP), including changes made pursuant to the authority of 10 CFR 50.90 and 10 CFR 50.54(p). The licensee's CSP was approved by License Amendment No. 226.

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

(1) DELETED



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

CAROLINA POWER & LIGHT COMPANY, et al.

DOCKET NO. 50-400

SHEARON HARRIS NUCLEAR POWER PLANT, UNIT 1

AMENDMENT TO RENEWED FACILITY OPERATING LICENSE

Amendment No. 136
Renewed License No. NPF-63

1. The Nuclear Regulatory Commission (the Commission) has found that:
 - A. The application for amendment by Carolina Power & Light Company (the licensee), dated July 8, 2011, as supplemented by letters dated September 23 and November 30, 2010; February 28 and April 7, 2011, complies with the standards and requirements of the Atomic Energy Act of 1954, as amended (the Act), and the Commission's rules and regulations set forth in Title 10 of the *Code of Federal Regulations* (10 CFR) Chapter I;
 - B. The facility will operate in conformity with the application, the provisions of the Act, and the rules and regulations of the Commission;
 - C. There is reasonable assurance (i) that the activities authorized by this amendment can be conducted without endangering the health and safety of the public, and (ii) that such activities will be conducted in compliance with the Commission's regulations;
 - D. The issuance of this amendment will not be inimical to the common defense and security or to the health and safety of the public; and
 - E. The issuance of this amendment is in accordance with 10 CFR Part 51 of the Commission's regulations and all applicable requirements have been satisfied.

2. Accordingly, the license is amended as indicated in the attachment to this license amendment, and paragraph 2.C.(2) of Facility Operating License No. NPF-63 is hereby amended to read as follows:

- (2) Technical Specifications and Environmental Protection Plan

The Technical Specifications contained in Appendix A, and the Environmental Protection Plan contained in Appendix B, both of which are attached hereto, as revised through Amendment No. 136, are hereby incorporated into this license. Carolina Power & Light Company shall operate the facility in accordance with the Technical Specifications and the Environmental Protection Plan.

3. In addition, Paragraph 2.E of Renewed Facility Operating License No. NPF-63 is revised to add the following language:

The licensee shall fully implement and maintain in effect all provisions of the Commission-approved cyber security plan (CSP), including changes made pursuant to the authority of 10 CFR 50.90 and 10 CFR 50.54(p). The licensee's CSP was approved by License Amendment No. 136.

4. This license amendment is effective as of the date of its issuance. The implementation of the CSP, including the key intermediate milestone dates and the full implementation date, shall be in accordance with the implementation schedule submitted by the licensee on April 7, 2011, and approved by the NRC staff with this license amendment. All subsequent changes to the NRC-approved CSP implementation schedule will require prior NRC approval pursuant to 10 CFR 50.90.

FOR THE NUCLEAR REGULATORY COMMISSION



Douglas A. Broaddus, Chief
Plant Licensing Branch II-2
Division of Operating Reactor Licensing
Office of Nuclear Reactor Regulation

Attachment:
Changes to the Renewed
License No. NPF-63

Date of Issuance: July 29, 2011

ATTACHMENT TO LICENSE AMENDMENT NO. 136

FACILITY OPERATING LICENSE NO. NPF-63

DOCKET NO. 50-400

Replace the following pages of Renewed Facility Operating License No. NPF-63 with the attached revised pages. The revised pages are identified by amendment number and contain marginal lines indicating the areas of change.

Remove Pages

4
8

Insert Pages

4
8
8a

C. This license shall be deemed to contain and is subject to the conditions specified in the Commission's regulations set forth in 10 CFR Chapter I and is subject to all applicable provisions of the Act and to the rules, regulations, and orders of the Commission now or hereafter in effect, and is subject to the additional conditions specified or incorporated below.

(1) Maximum Power Level

Carolina Power & Light Company is authorized to operate the facility at reactor core power levels not in excess of 2900 megawatts thermal (100 percent rated core power) in accordance with the conditions specified herein.

(2) Technical Specifications and Environmental Protection Plan

The Technical Specifications contained in Appendix A and the Environmental Protection Plan contained in Appendix B, both of which are attached hereto, as revised through Amendment No. 136, are hereby incorporated into this license. Carolina Power & Light Company shall operate the facility in accordance with the Technical Specifications and the Environmental Protection Plan.

(3) Antitrust Conditions

Carolina Power & Light Company shall comply with the antitrust conditions delineated in Appendix C to this license.

(4) Initial Startup Test Program (Section 14)¹

Any changes to the Initial Test Program described in Section 14 of the FSAR made in accordance with the provisions of 10 CFR 50.59 shall be reported in accordance with 50.59(b) within one month of such change.

(5) Steam Generator Tube Rupture (Section 15.6.3)

Prior to startup following the first refueling outage, Carolina Power & Light Company shall submit for NRC review and receive approval if a steam generator tube rupture analysis, including the assumed operator actions, which demonstrates that the consequences of the design basis steam generator tube rupture event for the Shearon Harris Nuclear Power Plant are less than the acceptance criteria specified in the Standard Review Plan, NUREG-0800, at '15.6.3 Subparts II(1) and (2) for calculated doses from radiological releases. In preparing their analysis Carolina Power & Light Company will not assume that operators will complete corrective actions within the first thirty minutes after a steam generator tube rupture.

¹The parenthetical notation following the title of many license conditions denotes the section of the Safety Evaluation Report and/or its supplements wherein the license condition is discussed.

E. Physical and Cyber Security

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.

The licensee shall fully implement and maintain in effect all provisions of the Commission-approved cyber security plan (CSP), including changes made pursuant to the authority of 10 CFR 50.90 and 10 CFR 50.54(p). The licensee's CSP was approved by License Amendment No. 136.

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.



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

FLORIDA POWER CORPORATION
CITY OF ALACHUA
CITY OF BUSHNELL
CITY OF GAINESVILLE
CITY OF KISSIMMEE
CITY OF LEESBURG
CITY OF NEW SMYRNA BEACH AND UTILITIES COMMISSION
CITY OF NEW SMYRNA BEACH
CITY OF OCALA
ORLANDO UTILITIES COMMISSION AND CITY OF ORLANDO
SEMINOLE ELECTRIC COOPERATIVE, INC.
DOCKET NO. 50-302
CRYSTAL RIVER UNIT 3 NUCLEAR GENERATING PLANT
AMENDMENT TO FACILITY OPERATING LICENSE

Amendment No. 238
License No. DPR-72

1. The Nuclear Regulatory Commission (the Commission) has found that:
 - A. The application for amendment by Florida Power Corporation, et al. (the licensees), dated July 8, 2011, as supplemented by letters dated September 23 and November 30, 2010; February 28 and April 7, 2011, complies with the standards and requirements of the Atomic Energy Act of 1954, as amended (the Act), and the Commission's rules and regulations set forth in Title 10 of the *Code of Federal Regulations* (10 CFR) Chapter I;
 - B. The facility will operate in conformity with the application, the provisions of the Act, and the rules and regulations of the Commission;
 - C. There is reasonable assurance (i) that the activities authorized by this amendment can be conducted without endangering the health and safety of the public, and (ii) that such activities will be conducted in compliance with the Commission's regulations;
 - D. The issuance of this amendment will not be inimical to the common defense and security or to the health and safety of the public; and

- E. The issuance of this amendment is in accordance with 10 CFR Part 51 of the Commission's regulations and all applicable requirements have been satisfied.
2. Accordingly, the license is amended as indicated in the attachment to this license amendment, and paragraph 2.C.(2) of Facility Operating License No. DPR-72 is hereby amended to read as follows:

Technical Specifications

The Technical Specifications contained in Appendices A and B, as revised through Amendment No. 238 , are hereby incorporated in the license. Florida Power Corporation shall operate the facility in accordance with the Technical Specifications.

3. In addition, Paragraph 2.D of Facility Operating License No. DPR-72 is revised to add the following language:

The licensee shall fully implement and maintain in effect all provisions of the Commission-approved cyber security plan (CSP), including changes made pursuant to the authority of 10 CFR 50.90 and 10 CFR 50.54(p).
The licensee's CSP was approved by License Amendment No. 238 .

4. This license amendment is effective as of the date of its issuance. The implementation of the CSP, including the key intermediate milestone dates and the full implementation date, shall be in accordance with the implementation schedule submitted by the licensee on April 7, 2011, and approved by the NRC staff with this license amendment. All subsequent changes to the NRC-approved CSP implementation schedule will require prior NRC approval pursuant to 10 CFR 50.90.

FOR THE NUCLEAR REGULATORY COMMISSION



Douglas A. Broaddus, Chief
Plant Licensing Branch II-2
Division of Operating Reactor Licensing
Office of Nuclear Reactor Regulation

Attachment:
Changes to License No. DPR-72

Date of Issuance: July 29, 2011

ATTACHMENT TO LICENSE AMENDMENT NO. 238

FACILITY OPERATING LICENSE NO. DPR-72

DOCKET NO. 50-302

Replace the following pages of Facility Operating License DPR-72 with the attached revised pages. The revised pages are identified by amendment number and contain vertical lines indicating the areas of change.

Remove Pages

4
5d

Insert Pages

4
5d

of the Act and to the rules, regulations, and orders of the Commission now or hereafter in effect; and is subject to the additional conditions specified or incorporated below:

2.C.(1) Maximum Power Level

Florida Power Corporation is authorized to operate the facility at a steady state reactor core power level not in excess of 2609 Megawatts (100 percent of rated core power level).

2.C.(2) Technical Specifications

The Technical Specifications contained in Appendices A and B, as revised through Amendment No. 238, are hereby incorporated in the license. Florida Power Corporation shall operate the facility in accordance with the Technical Specifications.

The Surveillance Requirements contained in the Appendix A Technical Specifications and listed below are not required to be performed immediately upon implementation of Amendment 149. The Surveillance Requirements shall be successfully demonstrated prior to the time and condition specified below for each.

- a) SR 3.3.8.2.b shall be successfully demonstrated prior to entering MODE 4 on the first plant start-up following Refuel Outage 9.
- b) SR 3.3.11.2, Function 2, shall be successfully demonstrated no later than 31 days following the implementation date of the ITS.
- c) SR 3.3.17.1, Functions 1, 2, 6, 10, 14, & 17 shall be successfully demonstrated no later than 31 days following the implementation date of the ITS.
- d) SR 3.3.17.2, Function 10 shall be successfully demonstrated prior to entering MODE 3 on the first plant start-up following Refuel Outage 9.
- e) SR 3.6.1.2 shall be successfully demonstrated prior to entering MODE 2 on the first plant start-up following Refuel Outage 9.
- f) SR 3.7.12.2 shall be successfully demonstrated prior to entering MODE 2 on the first plant start-up following Refuel Outage 9.
- g) SR 3.8.1.10 shall be successfully demonstrated prior to entering MODE 2 on the first plant start-up following Refuel Outage 9.
- h) SR 3.8.3.3 shall be successfully demonstrated prior to entering MODE 4 on the first plant start-up following Refuel Outage 9.

2.D Physical and Cyber Security

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 2781.7 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 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 licensee shall fully implement and maintain in effect all provisions of the Commission-approved cyber security plan (CSP), including changes made pursuant to the authority of 10 CFR 50.90 and 10 CFR 50.54(p). The licensee's CSP was approved by License Amendment No. 238.



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

SAFETY EVALUATION BY THE OFFICE OF NUCLEAR REACTOR REGULATION

RELATED TO THE FOLLOWING:

AMENDMENT NOS. 258 AND 286

RENEWED FACILITY OPERATING LICENSE NOS. DPR-71 AND DPR-62

BRUNSWICK STEAM ELECTRIC PLANT, UNITS. 1 AND 2

DOCKET NOS. 50-325, AND 50-324

AMENDMENT NO. 226

RENEWED FACILITY OPERATING LICENSE NO. DPR-23

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

DOCKET NO. 50-261

AMENDMENT NO. 136

RENEWED FACILITY OPERATING LICENSE NO. NPF-63

SHEARON HARRIS NUCLEAR POWER PLANT, UNIT 1

DOCKET NO. 50-400

AMENDMENT NO. 238

FACILITY OPERATING LICENSE NO. DPR-72

CRYSTAL RIVER UNIT 3 NUCLEAR GENERATING PLANT

DOCKET NO. 50-302

1.0 INTRODUCTION

By letter dated July 8, 2010 (Agencywide Documents Access and Management System (ADAMS) Accession No. ML1019500343), as supplemented by letters dated September 23 and November 30, 2010, February 28 and April 7, 2011 (ADAMS Accession Nos. ML102720415, ML103410162, ML110670686, ML11108A022, respectively), Carolina Power & Light and Florida Power Corporation (the licensees) submitted a license amendment request for approval of the licensees' cyber security plan (CSP) and its implementation schedule for Brunswick Steam Electric Plant (BSEP), Units 1 and 2, H. B. Robinson Steam Electric Plant, Unit No. 2 (RSEP-2), Shearon Harris Nuclear Power Plant, Unit 1 (HNP-1) and Crystal River Unit 3

Nuclear Generating Plant (CR-3), as required by Title 10 of the *Code of Federal Regulations* (10 CFR) 73.54 (Reference 1). The licensees' submittals dated November 30, 2010, and April 7, 2011, supplemented the licensees' CSP to address: 1) scope of systems in response to the October 21, 2010, Nuclear Regulatory Commission (NRC, Commission) decision (Reference 2); 2) records retention; and 3) implementation schedule. In its letter dated April 7, 2011, the licensees provided a revised copy of the licensees' "Cyber Security Plan," Revision 0 that incorporated all of the changes that the licensees had made to the following sections of their CSP: Scope and Purpose, Defense-In-Depth Protective Strategies, Document Control and Records Retention and Handling, and Deviations From Nuclear Energy Institute (NEI) 08-09, "Cyber Security Plan for Nuclear Power Reactors," Revision 6.

The September 23 and November 30, 2010, and February 28, 2011, supplements and the Updated No Significant Hazards Consideration in Enclosure 5 of the letter dated April 7, 2011, contained clarifying information and did not change the NRC's initial proposed finding of no significant hazards consideration.

2.0 REGULATORY EVALUATION

2.1 General Requirements

Consistent with 10 CFR 73.54(a), the licensee must 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 (DBT), as described in 10 CFR 73.1. The licensee 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 (SSEP) functions. The rule specifies that digital computer and communication systems and networks associated with these functions must be protected from cyber attacks that would adversely impact the integrity or confidentiality of data and software; deny access to systems, services, or data; or provide an adverse impact to the operations of systems, networks, and associated equipment.

In the October 21, 2010, Staff Requirements Memorandum (SRM)-COMWCO-10-0001 (Reference 2), the NRC stated that the NRC's cyber security rule at 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. The NRC staff determined that SSCs in the BOP that have a nexus to radiological health and safety are those that could directly or indirectly affect reactivity of a nuclear power plant (NPP), and are therefore within the scope of important-to-safety functions described in 10 CFR 73.54(a)(1).

2.2 Elements of a CSP

As stated in 10 CFR 73.54(e), the licensee must establish, implement, and maintain a CSP that satisfies the Cyber Security Program requirements of this regulation. In addition, the CSP must describe how the licensee will implement the requirements of the regulation and must account for the site-specific conditions that affect implementation. One method of complying with this

regulation is to describe within the CSP how the licensee will achieve high assurance that all SSEP functions are protected from cyber attacks.

2.3 Regulatory Guide 5.71 and NEI 08-09, Revision 6

Regulatory Guide (RG) 5.71, "Cyber Security Programs for Nuclear Facilities," (Reference 3) describes a regulatory position that promotes a defensive strategy consisting of a defensive architecture and a set of security controls based on standards provided in the National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53, "Recommended Security Controls for Federal Information Systems and Organizations," and NIST SP 800-82, "Guide to Industrial Control Systems Security," dated September 29, 2008. NIST SP 800-53 and NIST SP 800-82 are based on well-understood cyber threats, risks, and vulnerabilities, coupled with equally well-understood countermeasures and protective techniques. RG 5.71 divides the above-noted security controls into three broad categories: technical, operational, and management.

RG 5.71 provides a framework to aid in the identification of those digital assets that licensees must protect from cyber attacks. These identified digital assets are referred to as "critical digital assets" (CDAs). Licensees should address the potential cyber security risks to CDAs by applying the defensive architecture and addressing the collection of security controls identified in RG 5.71. RG 5.71 includes a CSP template that provides one method for preparing an acceptable CSP.

The organization of RG 5.71 reflects the steps necessary to meet the requirements of 10 CFR 73.54. Section C.3 of RG 5.71 describes an acceptable method for implementing the security controls, as detailed in Appendix B, "Technical Controls," and Appendix C, "Operational and Management Controls." Section C.4 of RG 5.71 discusses the need to maintain the established Cyber Security Program, including comprehensive monitoring of the CDAs and the effectiveness of their security protection measures, ensuring that changes to the CDAs or the environment are controlled, coordinated, and periodically reviewed for continued protection from cyber attacks. Section C.5 of RG 5.71 provides licensees and applicants with guidance for retaining records associated with their cyber security programs. Appendix A to RG 5.71 provides a template for a generic cyber security plan which licensees may use to comply with the licensing requirements of 10 CFR 73.54. Appendices B and C provide an acceptable set of security controls, which are based on well-understood threats, vulnerabilities, and attacks, coupled with equally well-understood and vetted countermeasures and protective techniques.

NEI 08-09, Revision 6 closely maps with RG 5.71; Appendix A of NEI 08-09, Revision 6 contains a cyber security plan template that is comparable to Appendix A of RG 5.71. Appendix D of NEI 08-09, Revision 6 contains technical cyber security controls that are comparable to Appendix B of RG 5.71. Appendix E of NEI 08-09, Revision 6 contains operational and management cyber security controls that are comparable to Appendix C of RG 5.71.

The NRC staff stated in a letter, dated May 5, 2010 (Reference 4), that licensees may use the template in NEI 08-09, Revision 6 (Reference 5), to prepare an acceptable CSP, with the exception of the definition of "cyber attack." The NRC staff subsequently reviewed and approved by letter dated June 7, 2010 (Reference 6), a definition for "cyber attack" for use by

licensees in their submissions based on NEI 08-09, Revision 6. The licensees' submittal dated April 7, 2011, included a CSP for the BSEP, Units 1 and 2; the CR-3; the RSEP-2, and the HNP-11; that was based on the template provided in NEI 08-09, Revision 6 and a definition of cyber attack acceptable to the NRC staff in CSP, Table 1, "Deviations from NEI 08-09, Revision 6." Additionally, the licensees supplement dated November 30, 2010, included information on SSCs in the BOP that, if compromised, could affect nuclear power plant reactivity.

RG 5.71 and NEI 08-09, Revision 6 are comparable documents; both are based on essentially the same general approach and same set of technical, operational, and management security controls. The submitted CSP was reviewed against the corresponding sections in RG 5.71.

3.0 TECHNICAL EVALUATION

The NRC staff performed a technical evaluation of the licensees' submittal. The licensees' submittal, with the exceptions of deviations described in Section 4.0, generally conformed to the guidance in NEI 08-09, Revision 6, which was found to be acceptable by the NRC staff and comparable to RG 5.71 to satisfy the requirements contained in 10 CFR 73.54.

3.1 Scope and Purpose

The licensees' CSP establishes a means to achieve high assurance that digital computer and communication systems and networks associated with the following functions are adequately protected against cyber attacks up to and including the DBT:

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 SSEP functions.

The submitted CSP describes achievement of high assurance of adequate protection of systems associated with the above functions from cyber attacks by:

- Implementing and documenting the "baseline" security controls as described in Section 3.1.6 of NEI 08-09, Revision 6, which is comparable to Regulatory Position C.3.3 described in RG 5.71; and
- Implementing and documenting a Cyber Security Program to maintain the established cyber security controls through a comprehensive life cycle approach as described in Section 4 of NEI 08-09, Revision 6, which is comparable to Appendix A, Section A.2.1 of RG 5.71.

Thus, the licensees' CSP, as originally submitted, is comparable to the CSP in NEI-08-09, Revision 6. However, in its submittal dated November 30, 2010, the licensees clarified its original submission and indicated that the scope of systems includes those BOP SSCs that

have an impact on NPP reactivity if compromised. This is in response to and consistent with SRM-COMWCO-10-0001, in which the Commission stated that the NRC's cyber security rule in 10 CFR 73.54 should be interpreted to include SSCs in the BOP that have a nexus to radiological health and safety. The staff determined that those systems that have a nexus to radiological health and safety are those that could directly or indirectly affect reactivity of a NPP, and are therefore within the scope of important-to-safety functions described in 10 CFR 73.54(a)(1).

The NRC staff reviewed the CSP and the supplemental information submitted by the licensees and found no deviation from Regulatory Position C.3.3 in RG 5.71 and Appendix A, Section A.2.1 of RG 5.71. The NRC staff finds that the licensees established adequate measures to implement and document the Cyber Security Program, including baseline security controls.

Based on the above, the NRC staff finds that the CSP adequately establishes the Cyber Security Program, including baseline security controls.

3.2 Analyzing Digital Computer Systems and Networks and Applying Cyber Security Controls

The licensees' CSP describes that the Cyber Security Program is established, implemented, and maintained as described in Section 3.1 of NEI 08-09, Revision 6, which is comparable to Regulatory Position C.3.1 described in RG 5.71 to:

- Analyze digital computer and communications systems and networks; and
- Identify those assets that must be protected against cyber attacks to satisfy 10 CFR 73.54(a).

The submitted CSP describes how the cyber security controls in Appendices D and E of NEI 08-09, Revision 6, which are comparable to Appendices B and C in RG 5.71, are addressed to protect CDAs from cyber attacks.

This section of the CSP submitted by the licensees is comparable to Regulatory Position C.3.1 in RG 5.71 without deviation.

Based on the above, the NRC staff finds that the CSP adequately addresses security controls.

3.3 Cyber Security Assessment and Authorization

The licensees provided information addressing the creation of a formal, documented, cyber security assessment and authorization policy. This included a description concerning the creation of a formal, documented procedure comparable to Section 3.1.1 of NEI 08-09, Revision 6.

The NRC staff finds that the licensees established adequate measures to define and address the purpose, scope, roles, responsibilities, management commitment, and coordination, and facilitates the implementation of the cyber security assessment and authorization policy.

The NRC staff reviewed the above information and found no deviation from Section 3.1.1 of NEI 08-09, Revision 6, which is comparable to Regulatory Position C.3.1.1 and Appendix A, Section A.3.1.1 of RG 5.71.

Based on the above, the NRC staff finds that the CSP adequately established controls to develop, disseminate, and periodically update the cyber security assessment and authorization policy and implementing procedure.

3.4 Cyber Security Assessment Team

The licensee's CSP establishes a Cyber Security Assessment Team (CSAT) whose responsibilities include conducting the cyber security assessment, documenting key findings during the assessment, and evaluating assumptions and conclusions about cyber security threats. The submitted CSP outlines the requirements, roles and responsibilities of the CSAT comparable to Section 3.1.2 of NEI 08-09, Revision 6. It also describes that the CSAT has the authority to conduct an independent assessment.

The submitted CSP describes that the CSAT will consist of individuals with knowledge about information and digital systems technology; NPP operations, engineering, and plant technical specifications; and physical security and emergency preparedness systems and programs. The CSAT description in the CSP is comparable to Regulatory Position C.3.1.2 in RG 5.71.

The submitted CSP lists the roles and responsibilities for the CSAT, which include: performing and overseeing the cyber security assessment process; documenting key observations; evaluating information about cyber security threats and vulnerabilities; confirming information obtained during tabletop reviews, walk-downs, or electronic validation of CDAs; and identifying potential new cyber security controls.

This section of the CSP submitted by the licensees is comparable to Regulatory Position C.3.1.2 in RG 5.71 without deviation.

Based on the above, the NRC staff finds that the CSP adequately establishes the requirements, roles and responsibilities of the CSAT.

3.5 Identification of CDAs

The submitted CSP describes that the licensees will identify and document CDAs and critical systems (CSs), including a general description, the overall function, the overall consequences if a compromise were to occur, and the security functional requirements or specifications as described in Section 3.1.3 of NEI 08-09, Revision 6, which is comparable to Regulatory Position C.3.1.3 of RG 5.71.

Based on the above, the NRC staff finds that the CSP adequately describes the process to identify CDAs.

3.6 Examination of Cyber Security Practices

The submitted CSP describes how the CSAT will examine and document the existing cyber security policies, procedures, and practices; existing cyber security controls; detailed descriptions of network and communication architectures (or network/communication architecture drawings); information on security devices; and any other information that may be helpful during the cyber security assessment process as described in Section 3.1.4 of NEI 08-09, Revision 6, which is comparable to Regulatory Position C.3.1.2 of RG 5.71. The examinations will include an analysis of the effectiveness of the existing Cyber Security Program and cyber security controls. The CSAT will document the collected cyber security information and the results of their examination of the collected information.

This section of the CSP submitted by the licensees is comparable to Regulatory Position C.3.1.2 in RG 5.71 without deviation.

Based on the above, the NRC staff finds that the CSP adequately describes the examination of cyber security practices.

3.7 Tabletop Reviews and Validation Testing

The submitted CSP describes tabletop reviews and validation testing, which confirm the direct and indirect connectivity of each CDA and identify direct and indirect pathways to CDAs. The CSP states that validation testing will be performed electronically or by physical walkdowns. The licensees' plan for tabletop reviews and validation testing is comparable to Section 3.1.5 of NEI 08-09, Revision 6, which is comparable to Regulatory Position C.3.1.4 of RG 5.71.

Based on the above, the NRC staff finds that the CSP adequately describes tabletop reviews and validation testing.

3.8 Mitigation of Vulnerabilities and Application of Cyber Security Controls

The submitted CSP describes the use of information collected during the cyber security assessment process (e.g., disposition of cyber security controls, defensive models, defensive strategy measures, site and corporate network architectures) to implement security controls in accordance with Section 3.1.6 of NEI 08-09, Revision 6, which is comparable to Regulatory Position C.3.3 and Appendix A.3.1.6 to RG 5.71. The CSP describes the process that will be applied in cases where security controls cannot be implemented.

The submitted CSP notes that before the licensees can implement security controls on a CDA, they will assess the potential for adverse impact in accordance with Section 3.1.6 of NEI 08-09, Revision 6, which is comparable to Regulatory Position C.3.3 of RG 5.71.

Based on the above, the NRC staff finds that the CSP adequately describes mitigation of vulnerabilities and application of security controls.

3.9 Incorporating the Cyber Security Program into the Physical Protection Program

The submitted CSP states that the Cyber Security Program will be reviewed as a component of the Physical Security Program in accordance with the requirements of 10 CFR 73.55(m). This is comparable to Section 4.1 of NEI 08-09, Revision 6, which is comparable to Regulatory Position C.3.4 of RG 5.71.

This section of the CSP submitted by the licensees is comparable to Appendix A, Section A.3.2 in RG 5.71 without deviation.

Based on the above, the NRC staff finds that the CSP adequately describes review of the CSP as a component of the physical security program.

3.10 Cyber Security Controls

The submitted CSP describes how the technical, operational and management cyber security controls contained in Appendices D and E of NEI 08-09, Revision 6, that are comparable to Appendices B and C in RG 5.71, are evaluated and dispositioned based on site-specific conditions during all phases of the Cyber Security Program. The CSP describes that many security controls have actions that are required to be performed on specific frequencies and that the frequency of a security control is satisfied if the action is performed within 1.25 times the frequency specified in the control, as applied, and as measured from the previous performance of the action as described in Section 4.2 of NEI 08-09, Revision 6.

This section of the CSP submitted by the licensees is comparable to Appendix A, Section A.3.1.6 in RG 5.71 without deviation.

Based on the above, the NRC staff finds that the CSP adequately describes implementation of cyber security controls.

3.11 Defense-in-Depth Protective Strategies

The submitted CSP describes the implementation of defensive strategies that ensure the capability to detect, respond to, and recover from a cyber attack. The CSP specifies that the defensive strategies consist of security controls, defense-in-depth measures, and the defensive architecture. The submitted CSP notes that the defensive architecture establishes the logical and physical boundaries to control the data transfer between these boundaries.

The licensees established defense-in-depth strategies by: implementing and documenting a defensive architecture as described in Section 4.3 of NEI 08-09, Revision 6, which is comparable to Regulatory Position C.3.2 in RG 5.71; a physical security program, including physical barriers; the operational and management controls described in Appendix E of NEI 08-09, Revision 6, which is comparable to Appendix C to RG 5.71; and the technical controls described in Appendix D of NEI 08-09, Revision 6, which is comparable to Appendix B to RG 5.71.

The NRC staff questioned how one-way communications will be restricted between two different security levels/zones to prevent any data transmission from the lower security level to the higher

security level. The licensees, by letter dated February 28, 2011, responded to the NRC staff's RAI and revised the CSP to state that 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 through the use of a firewall or network-based intrusion detection system.

The NRC staff also questioned how the bidirectional communications will be secured between voice and data communication networks that will prevent any data transmission to Level 3. The licensees, by letter dated February 28, 2011, responded to the NRC staff's RAI and clarified that they have multiple Level 3 type networks that have equivalent protective characteristics. Level 3 communications voice and data networks and Level 3 plant computer networks are separate networks based on the functions they support and are not directly connected to each other. Level 3 plant computer networks will be deterministically segregated from business computer networks by unidirectional network communications. These voice and data networks require bidirectional communication with less secure networks. Boundary security controls and interfaces are applied as determined by an evaluation in accordance with Section 3.1.6 of the CSP. The NRC staff finds that the licensees' defense-in-depth protective strategy as clarified ensures that only one-way data flow is allowed from Level 4 to Level 3 and from Level 3 to Level 2 and is consistent with the intent of Section 4.3 of NEI 08-09, Revision 6.

Based on the above discussions, this section of the CSP submitted by the licensees is comparable to Regulatory Position C.3.2 and Appendix A, Section A.3.1.5 in RG 5.71 without deviation. Based on the licensees' comprehensive defense-in-depth protective strategies providing the capability to detect, respond to, and recover from a cyber attack, the NRC staff finds that the CSP adequately describes implementation of defense-in-depth protective strategies.

3.12 Ongoing Monitoring and Assessment

The submitted CSP describes how ongoing monitoring of cyber security controls to support CDAs is implemented comparable to Appendix E of NEI 08-09, Revision 6, which is comparable to Regulatory Positions C.4.1 and C.4.2 of RG 5.71. The ongoing monitoring program includes configuration management and change control; cyber security impact analysis of changes and changed environments; ongoing assessments of cyber security controls; effectiveness analysis (to monitor and confirm that the cyber security controls are implemented correctly, operating as intended, and achieving the desired outcome) and vulnerability scans to identify new vulnerabilities that could affect the security posture of CDAs.

This section of the CSP submitted by the licensees is comparable to Regulatory Positions C.4.1 and C.4.2 of RG 5.71 without deviation.

Based on the above, the NRC staff finds that the CSP adequately describes ongoing monitoring and assessment.

3.13 Modification of Digital Assets

The submitted CSP describes how cyber security controls are established, implemented, and maintained to protect CDAs. These security controls ensure that modifications to CDAs are evaluated before implementation, and that the cyber security performance objectives are

maintained, and that acquired CDAs have cyber security requirements in place to achieve the site's Cyber Security Program objectives. This is comparable to Section 4.5 of NEI 08-09, Revision 6, which is comparable to Appendices A.4.2.5 and A.4.2.6 of RG 5.71.

Based on the above, the NRC staff finds that the CSP adequately describes modification of digital assets.

3.14 Attack Mitigation and Incident Response

The submitted CSP describes the process to ensure that SSEP functions are not adversely impacted due to cyber attacks in accordance with Section 4.6 of NEI 08-09, Revision 6, which is comparable to Appendix C, Section C.8 of RG 5.71. The CSP includes a discussion about creating incident response policy and procedures, and addresses training, testing and drills, incident handling, incident monitoring, and incident response assistance. It also describes identification, detection, and response to cyber attacks; and containment, eradication, and recovery activities that are comparable to Section 4.6 of NEI 08-09, Revision 6.

This section of the CSP submitted by the licensees is comparable to Appendix C, Section C.8 of RG 5.71 without deviation.

Based on the above, the NRC staff finds that the CSP adequately describes attack mitigation and incident response.

3.15 Cyber Security Contingency Plan

The submitted CSP describes creation of a cyber security contingency plan and policy that protects CDAs from the adverse impacts of a cyber attack described in Section 4.7 of NEI 08-09, Revision 6, which is comparable to Regulatory Position C.3.3.2.7 and Appendix C.9 of RG 5.71. The licensees' CSP describe a cyber security contingency plan that includes the response to events, procedures for operating CDAs in a contingency, roles and responsibilities of responders, processes and procedures for backup and storage of information, logical diagrams of network connectivity, current configuration information, and personnel lists for authorized access to CDAs.

This section of the CSP submitted by the licensees is comparable to Regulatory Position C.3.3.2.7 of RG 5.71 without deviation.

Based on the above, the NRC staff finds that the CSP adequately describes the cyber security contingency plan.

3.16 Cyber Security Training and Awareness

The submitted CSP describes a program that establishes the training requirements necessary for the licensees' personnel and contractors to perform their assigned duties and responsibilities in implementing the Cyber Security Program in accordance with Section 4.8 of NEI 08-09, Revision 6, which is comparable to Regulatory Position C.3.3.2.8 of RG 5.71.

The CSP states that individuals will be trained with a level of cyber security knowledge commensurate with their assigned responsibilities in order to provide high assurance that individuals are able to perform their job functions in accordance with Appendix E of NEI 08-09, Revision 6, which is comparable to Regulatory Position C.3.3.2.8 of RG 5.71 and describes three levels of training: awareness training, technical training, and specialized cyber security training.

Based on the above, the NRC staff finds that the CSP adequately describes the cyber security training and awareness.

3.17 Evaluate and Manage Cyber Risk

The submitted CSP describes how cyber risk is evaluated and managed utilizing site programs and procedures comparable to Section 4.9 of NEI 08-09, Revision 6, which is comparable to Regulatory Position C.4 and Appendix C, Section C.13 of RG 5.71. The CSP describes the Threat and Vulnerability Management Program, Risk Mitigation, Operational Experience Program, and the Corrective Action Program, and how each will be used to evaluate and manage risk.

This section of the CSP submitted by the licensees is comparable to Regulatory Position C.4 and Appendix C, Section C.13 of RG 5.71 without deviation.

Based on the above, the NRC staff finds that the CSP adequately describes evaluation and management of cyber risk.

3.18 Policies and Implementing Procedures

The CSP describes development and implementation of policies and procedures to meet security control objectives in accordance with Section 4.10 of NEI 08-09, Revision 6, which is comparable to Regulatory Position C.3.5 and Appendix A, Section A.3.3 of RG 5.71. This includes the process to document, review, approve, issue, use, and revise program policies and procedures.

The CSP also describes the licensees' procedures to establish specific responsibilities for positions described in Section 4.11 of NEI 08-09, Revision 6, which is comparable to Appendix C, Section C.10.10 of RG 5.71.

This section of the CSP submitted by the licensees is comparable to Regulatory Position C.3.5, Appendix A, Section A.3.3, and Appendix C, Section C.10.10 of RG 5.71 without deviation.

Based on the above, the NRC staff finds that the CSP adequately describes cyber security policies and implementing procedures.

3.19 Roles and Responsibilities

The submitted CSP describes the roles and responsibilities for qualified and experienced personnel, including the Cyber Security Program Sponsor, the Cyber Security Program Manager, Cyber Security Specialists, the Cyber Security Incident Response Team (CSIRT), and

other positions as needed. Specifically, the CSIRT, in accordance with the Incident Response Plan, initiates emergency action when required to safeguard CDAs from cyber security compromise and to assist with the eventual recovery of compromised systems. Implementing procedures establish roles and responsibilities for each of the cyber security roles in accordance with Section 4.11 of NEI 08-09, Revision 6, which is comparable to Regulatory Position C.3.1.2, Appendix A, Section A.3.1.2, and Appendix C, Section C.10.10 of RG 5.71.

Based on the above, the NRC staff finds that the CSP adequately describes cyber security roles and responsibilities.

3.20 Cyber Security Program Review

The submitted CSP describes how the Cyber Security Program establishes the necessary procedures to implement reviews of applicable program elements in accordance with Section 4.12 of NEI 08-09, Revision 6, which is comparable to Regulatory Position C.4.3 and Appendix A, Section A.4.3 of RG 5.71.

Based on the above, the NRC staff finds that the CSP adequately describes Cyber Security Program review.

3.21 Document Control and Records Retention and Handling

The submitted CSP, Enclosure 2 of the letter dated July 8, 2010, describes that the licensees have established the necessary measures and governing procedures to ensure that sufficient records of items and activities affecting cyber security are developed, reviewed, approved, issued, used, and revised to reflect completed work. The CSP described that superseded portions of certain records will be retained for at least 3 years after the record is superseded, while audit records will be retained for no less than 12 months in accordance with Section 4.13 of NEI 08-09, Revision 6. However, this NEI guidance does not fully comply with the requirements of 10 CFR 73.54.

In a letter to the NRC dated February 28, 2011 (Reference 7), NEI proposed additional guidance for licensees' use to develop records retention policies and procedures that would comply with 10 CFR 73.54. In a letter dated March 1, 2011 (Reference 8), the NRC indicated that it had no technical objection to the NEI additional guidance. The proposed guidance provided examples (without providing an all-inclusive list) of the records and supporting technical documentation that are needed to satisfy the requirements of 10 CFR 73.54. All records will be retained until the Commission terminates the license, and the licensee shall maintain superseded portions of these records for at least 3 years after the record is superseded, unless otherwise specified by the Commission. By retaining accurate and complete records and technical documentation until the license is terminated, inspectors, auditors, or assessors will have the ability to evaluate incidents, events, and other activities that are related to any of the cyber security elements described, referenced, and contained within the licensee's NRC-approved CSP. It will also allow the licensee to maintain the ability to detect and respond to cyber attacks in a timely manner, in the case of an event.

In their letter dated April 7, 2011, the licensees responded to the NRC staff's RAI on records retention issue using the guidance proposed by NEI in its letter dated February 28, 2011. The licensees provided their revised CSP in Enclosure 2 of this submittal.

Based on the above, the NRC staff finds that the licensees' revised CSP provides for adequate document control and records retention and will support the licensees' ability to detect and respond to cyber attacks. The NRC staff further finds that this section is comparable to Regulatory Position C.5 and Appendix A, Section A.5 of RG 5.71 without deviation. Accordingly, the NRC staff concludes that the licensees' CSP adequately describes cyber security document control and records retention and handling.

3.22 Implementation Schedule

The submitted CSP provides a proposed implementation schedule for the Cyber Security Program. In a letter dated February 28, 2011 (Reference 9), NEI sent to the NRC a template for licensees to use to submit their CSP implementation schedules, to which the NRC had no technical objection (Reference 10). These key milestones include:

- Establish the CSAT;
- Identify CSs and CDAs;
- Install a deterministic one-way device between lower level devices and higher level devices;
- Implement the security control "Access Control For Portable And Mobile Devices";
- Implement observation and identification of obvious cyber related tampering to existing insider mitigation rounds by incorporating the appropriate elements;
- Identify, document, and implement cyber security controls as per "Mitigation of Vulnerabilities and Application of Cyber Security Controls" for CDAs that could adversely impact the design function of physical security target set equipment; and
- Commence ongoing monitoring and assessment activities for those target set CDAs whose security controls have been implemented.

The licensees, in their letter dated April 7, 2011, provided a revised implementation schedule using the NEI template. The NRC staff considers this April 7, 2011, supplement the approved schedule as required by 10 CFR 73.54. Based on the provided schedule ensuring timely implementation of those protective measures that provide a higher degree of protection against radiological sabotage, the NRC staff concludes that the Cyber Security Program implementation schedule is satisfactory.

The NRC staff acknowledges that, in its submittal dated July 8, 2010, the licensees proposed several CSP milestone implementation dates as regulatory commitments. The NRC staff does not regard the CSP milestone implementation dates as regulatory commitments that can be changed unilaterally by the licensees, particularly in light of the regulatory requirement at 10 CFR 73.54, that "[i]mplementation of the licensees' cyber security program must be consistent with the approved schedule." As the NRC staff explained in its letter to all operating reactor licensees dated May 9, 2011 (Reference 11), the implementation of the plan, including the key intermediate milestone dates and the full implementation date, shall be in accordance with the implementation schedule submitted by the licensees and approved by the NRC. All subsequent changes to the NRC-approved CSP implementation schedule thus will require prior NRC approval pursuant in 10 CFR 50.90.

Based on the provided schedule ensuring timely implementation of those protective measures that provide a higher degree of protection against radiological sabotage, the NRC staff finds the Cyber Security Program implementation schedule is satisfactory.

3.23 License Condition

By letter dated July 8, 2010, as supplemented by the letter dated April 7, 2011, the licensees proposed to add a license condition to Renewed Facility Operating License Nos. DPR-71, DPR-62, DPR-23, and NPF 63, and Facility Operating License No. DPR-72 for BSEP, Units 1 and 2, RSEP-2, HNP-1 and CR-3, respectively, that requires the licensees to fully implement and maintain in effect all provisions of the NRC-approved CSP. The NRC staff modified the proposed wording of the license conditions described in the licensees' submittal dated July 8, 2010, as shown below.

The following paragraph is added to Paragraph 2.D of Renewed Facility Operating License No. DPR-71 for BSEP, Unit 1:

The licensee shall fully implement and maintain in effect all provisions of the Commission-approved cyber security plan (CSP), including changes made pursuant to the authority of 10 CFR 50.90 and 10 CFR 50.54(p). The licensee's CSP was approved by License Amendment No. 258.

The following paragraph is added to Paragraph 2.C.(6) of Renewed Facility Operating License No. DPR-62 for BSEP, Unit 2:

The licensee shall fully implement and maintain in effect all provisions of the Commission-approved cyber security plan (CSP), including changes made pursuant to the authority of 10 CFR 50.90 and 10 CFR 50.54(p). The licensee's CSP was approved by License Amendment No. 286.

The following paragraph is added to Paragraph 3.F of Renewed Facility Operating License No. DPR-23 for RSEP-2:

The licensee shall fully implement and maintain in effect all provisions of the Commission-approved cyber security plan (CSP), including changes made pursuant to

the authority of 10 CFR 50.90 and 10 CFR 50.54(p). The licensee's CSP was approved by License Amendment No. 226.

The following paragraph is added to Paragraph 2.E of Renewed Facility Operating License No. NPF-63-62 for HNP-1:

The licensee shall fully implement and maintain in effect all provisions of the Commission-approved cyber security plan (CSP), including changes made pursuant to the authority of 10 CFR 50.90 and 10 CFR 50.54(p). The licensee's CSP was approved by License Amendment No. 136.

The following paragraph is added to Paragraph 2.D of Facility Operating License No. DPR-72 for CR-3:

The licensee shall fully implement and maintain in effect all provisions of the Commission-approved cyber security plan (CSP), including changes made pursuant to the authority of 10 CFR 50.90 and 10 CFR 50.54(p). The licensee's CSP was approved by License Amendment No. 238.

Based on the information in Section 3.0 of this safety evaluation and the modified license condition described above, the NRC concludes this is acceptable.

4.0 DIFFERENCES FROM NEI 08-09, REVISION 6

The licensees, in Table 1 of Enclosure 2 to the letter dated April 7, 2011, documented the following deviations from NEI 08-09, Revision 6:

- As discussed in Section 2.0, "Regulatory Evaluation," the licensees included a definition of cyber attack that is acceptable to the NRC staff.
- As discussed in Section 3.1, "Scope and Purpose," the licensees clarified the definition of important-to-safety functions, consistent with SRM-COMWCO-10-0001.
- As discussed in Section 3.21, "Document Control and Records Retention and Handling," the licensees clarified the definition of records and supporting documentation that will be retained to conform to the requirements of 10 CFR 73.54.

The NRC staff finds the above deviations to be acceptable, as discussed in the respective sections.

The NRC staff notes the following additional difference between the licensee's April 7, 2011 submission, and NEI 08-09, Revision 6:

- The licensees submitted a revised implementation schedule as Enclosure 2 to the licensees' April 7, 2011 letter, which specifies the interim milestones and the final implementation date for the CSP, including supporting rationale.

The NRC staff finds the above difference from NEI 08-09, Revision 6 to be acceptable, as discussed in Section 3.22, "Implementation Schedule."

5.0 STATE CONSULTATION

In accordance with the Commission's regulations, the North Carolina official was notified of the proposed issuance of the amendments for BSEP Units 1 and 2 and HNP-1, and the South Carolina officials were notified of the proposed amendment for RSEP-2. The North Carolina and South Carolina State official had no comments.

Based upon a letter dated May 2, 2003, from Michael N. Stephens of the Florida Department of Health, Bureau of Radiation Control, to Brenda L. Mozafari, Senior Project Manager, U.S. Nuclear Regulatory Commission, the State of Florida does not desire notification of issuance of license amendments.

6.0 ENVIRONMENTAL CONSIDERATION

The amendments change a requirement with respect to installation or use of a facility component located within the restricted area as defined in 10 CFR Part 20. The NRC staff has determined that the amendments involve no significant increase in the amounts, and no significant change in the types, of any effluents that may be released offsite, and that there is no significant increase in individual or cumulative occupational radiation exposure. The Commission has previously issued a proposed finding that the amendments involve no significant hazards consideration, and there has been no public comment on such finding published in the *Federal Register* on October 12 2010 (75 FR 62595). Also, these amendments relate to safeguards matters and do not involve any significant construction impacts and relate to changes in recordkeeping, reporting, or administrative procedures or requirements. Accordingly, the amendments meet the eligibility criteria for categorical exclusion set forth in 10 CFR 51.22(c)(9), (10), and (12). Pursuant to 10 CFR 51.22(b), no environmental impact statement or environmental assessment need be prepared in connection with the issuance of the amendments.

7.0 CONCLUSION

The NRC staff's review and evaluation of the licensees' CSP was conducted using the NRC staff positions established in the relevant sections of RG 5.71. Based on its review, the NRC finds that the licensees addressed the relevant information necessary to satisfy the requirements of 10 CFR 73.54, 10 CFR 73.55(a)(1), 10 CFR 73.55(b)(8), and 10 CFR 73.55(m), as applicable and that the licensees' Cyber Security Program provides high assurance that digital computer and communication systems and networks are adequately protected against cyber attacks, up to and including the DBT as described in 10 CFR 73.1. This includes protecting 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 SSEP functions.

Therefore, the NRC staff finds the information contained in the submitted CSP acceptable and upon successful implementation of this program, operation of the Brunswick Steam Electric

Plant, Units 1 and 2; the H. B. Robinson Steam Electric Plant, Unit No. 2; the Shearon Harris Nuclear Power Plant, Unit 1; and the Crystal River Unit 3 Nuclear Generating Plant; will not be inimical to the common defense and security.

8.0 REFERENCES

1. Section 73.54 of 10 CFR, "Protection of Digital Computer and Communication Systems and Networks," NRC, Washington, DC, March 27, 2009 (74 FR 13927).
2. SRM-COMWCO-10-0001, "Regulation of Cyber Security at Nuclear Power Plants," October 21, 2010 (ADAMS Accession No. ML102940009).
3. RG 5.71, "Cyber Security Programs for Nuclear Facilities," NRC, Washington, DC, January 2010 (ADAMS Accession No. ML090340159).
4. Richard Correia, NRC, letter to Jack Roe, NEI, "Nuclear Energy Institute 08-09, 'Cyber Security Plan Template, Revision 6'," May 5, 2010 (ADAMS Accession No. ML101190371).
5. Jack Roe, NEI, letter to Scott Morris, NRC, "NEI 08-09, Revision 6, 'Cyber Security Plan for Nuclear Power Reactors; April 2010,'" April 28, 2010 (ADAMS Accession No. ML101180434).
6. Richard P. Correia, NRC, letter to Christopher E. Earls, NEI, "Nuclear Energy Institute 08-09, 'Cyber Security Plan Template, Rev. 6'," June 7, 2010 (ADAMS Accession No. ML101550052).
7. Christopher E. Earls, NEI, letter to Richard P. Correia, NRC, "Clarification to NEI 08-09, Revision 6 Regarding Records Retention," February 28, 2011 (ADAMS Accession No. ML110600204).
8. Richard P. Correia, NRC, letter to Christopher E. Earls, NEI, "Template for The Cyber Security Plan request for Additional Information on Records Retention," March 1, 2011 (ADAMS Accession No. ML110400337).
9. Christopher E. Earls, NEI, letter to Richard P. Correia, NRC, "Template for the Cyber Security Plan Implementation Schedule," February 28, 2011 (ADAMS Accession No. ML110600206).
10. Richard P. Correia, NRC, letter to Christopher E. Earls, NEI, "Template for the Cyber Security Plan Implementation Schedule," March 1, 2011 (ADAMS Accession No. ML110070348).

11. Robert J. Pascarelli, NRC, to Holders of Licenses for Operating Power Reactors listed in the Enclosure, "Cyber Security Plan Implementation Schedule," May 9, 2011 (ADAMS Accession No. ML110980538)

Principal Contributor: Monika Coflin

Dated: July 29, 2011

of this program, operation of the BSEP, Units 1 and 2, RSEP- 2, HNP-1, and CR-3 will not be inimical to the common defence and security.

The amendments approve the licensees' proposed cyber security plans and associated implementation schedule; revise Renewed Facility Operating License Nos. DPR-71, DPR-62, DPR-23; NPF 63, for BSEP, Unit Nos. 1 and 2, RBSEP-2, and HNP-1, respectively, and Facility Operating License No. DPR-72 for CR-3; and add a license condition to require the licensees to fully implement and maintain in effect all provisions of the NRC-approved Cyber Security Plan.

A copy of the NRC staff related safety evaluation (SE) is enclosed. The enclosed SE was reviewed in accordance with the guidance provided in 10 CFR 2.390, and the NRC Staff has determined that no security-related or proprietary information is contained therein. The Notice of Issuance will be included in the Commission's next biweekly *Federal Register* notice. 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

Enclosures:

1. Amendment No. 258 to DPR-71
2. Amendment No. 286 to DPR-62
3. Amendment No. 226 to DPR-23
4. Amendment No. 136 to NPF-63
5. Amendment No. 238 to DPR-72
6. Safety Evaluation

cc: Distribution via Listserv

DISTRIBUTION:

PUBLIC	RidsNrrDorlLpl2-2	RidsNrrLACSola	T. Wengert, NRR
RidsNrrDorlDpr	RidsOgcRp	RidsRgn2MailCenter	C. Erlanger, NSIR
RidsAcrsAcnw_MailCTR	RidsNrrPMShearonHarris	B. Singal, NRR	RidsOgcRp
RidsNrrPMRobinson	RidsNrrPMCystalRiver	P. Pederson, NSIR	RidsNsirDsp
RidsNrrPMBrunswick	RidsNrrDorl	M. Coflin, NRR	LPL2-2 R/F

ADAMS Accession No.: ML11193A028

* By memo and email

OFFICE	LPL2-2/PM	LPL2-2/PM	LPL2-2/LA	NSIR/DSP/CSIRB/BC*
NAME	FSaba	BMOzafari	CSola	CErlanger*
DATE	07/14/11	07/29/11	07/14/11	06/23/11 07/09/11 (supplement)
OFFICE	OGC NLO	LPL2-2/BC	LPL2-2/PM	
NAME	AJones (w/ comments)	DBroaddus	FSaba	
DATE	07/25/11	07/29/11	07/29/11	