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

July 28, 2011

Mr. Thomas Joyce
President and Chief Nuclear Officer
PSEG Nuclear LLC
P.O. Box 236, N09
Hancocks Bridge, NJ 08038

SUBJECT: HOPE CREEK GENERATING STATION AND SALEM NUCLEAR GENERATING STATION, UNIT NOS. 1 AND 2 - ISSUANCE OF AMENDMENTS RE: APPROVAL OF CYBER SECURITY PLAN (TAC NOS. ME4352, ME4353 AND ME4354)

Dear Mr. Joyce:

The Commission has issued the enclosed Amendment No. 189 to Renewed Facility Operating License (FOL) No. NPF-57 for the Hope Creek Generating Station (HCGS) and Amendment Nos. 300 and 283 to Renewed FOL Nos. DPR-70 and DPR-75 for the Salem Nuclear Generating Station (Salem), Unit Nos. 1 and 2, in response to your application dated July 14, 2010, as supplemented by letters dated September 28, 2010, April 1, 2011, June 6, 2011, and July 6, 2011.

The amendments approve the Cyber Security Plan (CSP) and associated implementation schedule for HCGS and Salem Unit Nos. 1 and 2. In addition, the amendments revise the existing license condition regarding physical protection in the each of the three FOLs to require the licensee to fully implement and maintain in effect all provisions of the Nuclear Regulatory Commission (NRC)-approved CSP. The amendment requests were submitted pursuant to Section 73.54 of Title 10 of the *Code of Federal Regulations* (10 CFR) which requires licensees currently licensed to operate a nuclear power plant under 10 CFR Part 50 to submit a CSP for NRC review and approval.

A copy of our safety evaluation is also enclosed. Notice of Issuance will be included in the Commission's biweekly *Federal Register* notice.

Sincerely,

Richard B. Ennis, Senior Project Manager
Plant Licensing Branch I-2
Division of Operating Reactor Licensing
Office of Nuclear Reactor Regulation

Docket Nos. 50-354, 50-272, and 50-311

Enclosures:
1. Amendment No. 189 to
   Renewed License No. NPF-57
2. Amendment No. 300 to
   Renewed License No. DPR-70
3. Amendment No. 283 to
   Renewed License No. DPR-75
4. Safety Evaluation

cc w/encls: Distribution via ListServ

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

PSEG NUCLEAR LLC

DOCKET NO. 50-354

HOPE CREEK GENERATING STATION

AMENDMENT TO RENEWED FACILITY OPERATING LICENSE

Amendment No. 189
Renewed License No. NPF-57

1. The Nuclear Regulatory Commission (the Commission) has found that:

   A. The application for amendment filed by PSEG Nuclear LLC dated July 14, 2010, as supplemented by letters dated September 28, 2010, April 1, 2011, June 6, 2011, and July 6, 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 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 set forth in 10 CFR Chapter I;

   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, paragraph 2.E of Renewed Facility Operating License No. NPF-57 is hereby amended to add the following text:

   PSEG Nuclear LLC 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 Salem-Hope Creek CSP was approved by License Amendment No. 189.

3. This license amendment is effective as of the date of its issuance. The implementation of the Cyber Security Plan (CSP), including the key intermediate milestone dates and the full implementation date, shall be in accordance with the implementation schedule submitted by the licensee by letter dated June 6, 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

Harold K. Chernoff, Chief
Plant Licensing Branch I-2
Division of Operating Reactor Licensing
Office of Nuclear Reactor Regulation

Attachment:
Changes to the License

Date of Issuance: July 28, 2011

ATTACHMENT TO LICENSE AMENDMENT NO. 189

RENEWED FACILITY OPERATING LICENSE NO. NPF-57

DOCKET NO. 50-354

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

| Remove | Insert |
|---|---|
| Page 16 | Page 16 |
| - - - | Page 17 |

exempting Type C testing for instrument lines and lines containing excess flow check valves (Section 6.2.6 of SSER 5); and an exemption from Appendix J, exempting Type C testing of thermal relief valves (Section 6.2.6 of SSER 5). These exemptions are authorized by law, will not present an undue risk to the public health and safety, and are consistent with the common defense and security. These exemptions are hereby granted. The special circumstances regarding each exemption are identified in the referenced section of the safety evaluation report and the supplements thereto. These exemptions are granted pursuant to 10 CFR 50.12. With these exemptions, the facility will operate, to the extent authorized herein, in conformity with the application, as amended, the provisions of the Act, and the rules and regulations of the Commission.

E. 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, submitted by letter dated May 19, 2006 are entitled: "Salem-Hope Creek Nuclear Generating Station Security Training and Qualification Plan," and "Salem-Hope Creek Nuclear Generating Station Security Contingency Plan." The plans contain Safeguards Information protected under 10 CFR 73.21.

PSEG Nuclear LLC 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 Salem-Hope Creek CSP was approved by License Amendment No. 189.

F. DELETED

G. The licensees shall have and maintain financial protection of such type and in such amounts as the Commission shall require in accordance with Section 170 of the Atomic Energy Act of 1954, as amended, to cover public liability claims.

H. This renewed license is effective as of the date of issuance and shall expire at midnight on April 11, 2046.

FOR THE NUCLEAR REGULATORY COMMISSION

- original signed by E. J. Leeds -

Eric J. Leeds, Director
Office of Nuclear Reactor Regulation

Enclosures:
1. Appendix A - Technical Specifications (NUREG-1202)
2. Appendix B - Environmental Protection Plan
3. Appendix C - Additional Conditions

Date of Issuance: July 20, 2011

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

PSEG NUCLEAR LLC

EXELON GENERATION COMPANY, LLC

DOCKET NO. 50-272

SALEM NUCLEAR GENERATING STATION, UNIT NO. 1

AMENDMENT TO RENEWED FACILITY OPERATING LICENSE

Amendment No. 300
Renewed License No. DPR-70

1. The Nuclear Regulatory Commission (the Commission) has found that:

   A. The application for amendment filed by PSEG Nuclear LLC, acting on behalf of itself and Exelon Generation Company, LLC (the licensees) dated July 14, 2010, as supplemented by letters dated September 28, 2010, April 1, 2011, June 6, 2011, and July 6, 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 set forth in 10 CFR Chapter I;

   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, paragraph 2.E of Renewed Facility Operating License No. DPR-70 is hereby amended to add the following text:

   PSEG Nuclear LLC 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 Salem-Hope Creek CSP was approved by License Amendment No. 300.

3. This license amendment is effective as of the date of its issuance. The implementation of the Cyber Security Plan (CSP), including the key intermediate milestone dates and the full implementation date, shall be in accordance with the implementation schedule submitted by the licensee by letter dated June 6, 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

Harold K. Chernoff, Chief
Plant Licensing Branch I-2
Division of Operating Reactor Licensing
Office of Nuclear Reactor Regulation

Attachment:
Changes to the License

Date of Issuance: July 28, 2011

ATTACHMENT TO LICENSE AMENDMENT NO. 300

RENEWED FACILITY OPERATING LICENSE NO. DPR-70

DOCKET NO. 50-272

Replace the following page of Renewed Facility Operating License No. DPR-70 with the attached revised page as indicated. The revised page is identified by amendment number and contains a marginal line indicating the area of change.

| Remove | Insert |
| --- | --- |
| Page 9 | Page 9 |

evaluates such changes pursuant to the criteria set forth in 10 CFR 50.59 and otherwise complies with the requirements in that section.

(19) Appendix A of NUREG-2101, "Safety Evaluation Report Related to the License Renewal of Salem Nuclear Generating Station," dated June 2011, and PSEG Nuclear LLC UFSAR supplement submitted pursuant to 10 CFR 54.21(d), as revised on May 18, 2011, describe certain future programs and activities to be completed before the period of extended operation. PSEG Nuclear LLC shall complete these activities no later than August 13, 2016, and shall notify the NRC in writing when implementation of these activities is complete.

(20) All capsules in the reactor vessel that are removed and tested must meet the test procedures and reporting requirements of American Society for Testing and Materials (ASTM) E 185-82 to the extent practicable for the configuration of the specimens in the capsule. Any changes to the capsule withdrawal schedule, including spare capsules, must be approved by the NRC prior to implementation. All capsules placed in storage must be maintained for future insertion. Any changes to storage requirements must be approved by the NRC. Changes to the withdrawal schedule or storage requirements shall be submitted to the NRC as a report in accordance with 10 CFR 50.4.

(21) PSEG Nuclear LLC shall take one core sample in the Unit 1 spent fuel pool west wall, by the end of 2013, and one core sample in the east wall where there have been indications of borated water ingress through the concrete, by the end of 2015. The core samples (east and west walls) will expose the rebar, which will be examined for signs of corrosion. Any sample showing signs of concrete degradation and/or rebar corrosion will be entered into the licensee's corrective action program for further evaluation. PSEG Nuclear LLC shall submit a report in accordance with 10 CFR 50.4 no later than three months after each sample is taken on the results, recommendations, and any additional planned actions.

D. Paragraph 2.D. has been combined with paragraph 2.E. per Amendment No. 86, June 27, 1988.

E. 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, submitted by letter dated May 19, 2006, are entitled: "Salem-Hope Creek Nuclear Generating Station Security Plan," "Salem-Hope Creek Nuclear Generating Station Security Training and Qualification Plan," and "Salem-Hope Creek Nuclear Generating Station Security Contingency Plan." The plans contain Safeguards Information protected under 10 CFR 73.21.

PSEG Nuclear LLC 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 Salem-Hope Creek CSP was approved by License Amendment No. 300.

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

PSEG NUCLEAR LLC

EXELON GENERATION COMPANY, LLC

DOCKET NO. 50-311

SALEM NUCLEAR GENERATING STATION, UNIT NO. 2

AMENDMENT TO RENEWED FACILITY OPERATING LICENSE

Amendment No. 283
Renewed License No. DPR-75

1. The Nuclear Regulatory Commission (the Commission) has found that:

   A. The application for amendment filed by PSEG Nuclear LLC, acting on behalf of itself and Exelon Generation Company, LLC (the licensees) dated July 14, 2010, as supplemented by letters dated September 28, 2010, April 1, 2011, June 6, 2011, and July 6, 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 set forth in 10 CFR Chapter I;

   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, paragraph 2.E of Renewed Facility Operating License No. DPR-75 is hereby amended to add the following text:

   PSEG Nuclear LLC 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 Salem-Hope Creek CSP was approved by License Amendment No. 283.

3. This license amendment is effective as of the date of its issuance. The implementation of the Cyber Security Plan (CSP), including the key intermediate milestone dates and the full implementation date, shall be in accordance with the implementation schedule submitted by the licensee by letter dated June 6, 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

Harold K. Chernoff, Chief
Plant Licensing Branch I-2
Division of Operating Reactor Licensing
Office of Nuclear Reactor Regulation

Attachment:
Changes to the License

Date of Issuance: July 28, 2011

ATTACHMENT TO LICENSE AMENDMENT NO. 283

RENEWED FACILITY OPERATING LICENSE NO. DPR-75

DOCKET NO. 50-311

Replace the following page of Renewed Facility Operating License No. DPR-75 with the attached revised page as indicated. The revised page is identified by amendment number and contains a marginal line indicating the area of change.

| Remove | Insert |
| --- | --- |
| Page 11 | Page 11 |

issuance of the License for Fuel-Loading and Low-Power Testing, dated April 18, 1980. The facility will operate, to the extent authorized herein, in conformity with the application as amended, the provisions of the Act, and the regulations of the Commission.

E. 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, submitted by letter dated May 19, 2006, are entitled: "Salem-Hope Creek Nuclear Generating Station Security Plan," "Salem-Hope Creek Nuclear Generating Station Security Training and Qualification Plan," and "Salem-Hope Creek Nuclear Generating Station Security Contingency Plan." The plans Contain Safeguards Information protected under 10 CFR 73.21.

PSEG Nuclear LLC 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 Salem-Hope Creek CSP was approved by License Amendment No. 283.

F. A temporary exemption from General Design Criterion 57 found in Appendix A to 10 CFR Part 50 is described in the Office of Nuclear Reactor Regulation's Safety Evaluation Report, Supplement No. 5, Section 6.2.3.1. This Exemption is authorized by law and will not endanger life or property or the common defense and security and is otherwise in the public interest. The exemption, therefore, is hereby granted and shall remain in effect through the first refueling outage as discussed in Section 6.2.3.1 of Supplement 5 to the Safety Evaluation Report. The granting of the exemption is authorized with the issuance of the Facility Operating License, dated May 20, 1981. The facility will operate, to the extent authorized herein, in conformity with the application as amended, the provisions of the Act, and the regulations of the Commission.

G. This renewed license is subject to the following additional condition for the protection of the environment:

Before engaging in additional construction or operational activities which may result in an environmental impact that was not evaluated by the Commission, PSEG Nuclear LLC shall prepare and record an environmental evaluation of such activity. When the evaluation indicates that such activity may result in a significant adverse environmental impact that was not evaluated, or that is significantly greater than that evaluated in the Final Environmental Statement or any addendum thereto, PSEG Nuclear LLC shall provide a written evaluation of such activities and obtain prior approval from the Director of Nuclear Reactor Regulation.

H. If PSEG Nuclear LLC plans to remove or to make significant changes in the normal operation of equipment that controls the amount of radioactivity in effluents from the Salem Nuclear Generation Station, the NRC shall be notified in writing regardless of whether the change affects the amount of radioactivity in effluents.

I. DELETED

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

SAFETY EVALUATION BY THE OFFICE OF NUCLEAR REACTOR REGULATION

RELATED TO AMENDMENT NOS. 189, 300 AND 283

TO RENEWED FACILITY OPERATING LICENSE NOS. NPF-57, DPR-70, AND DPR-75

PSEG NUCLEAR LLC

HOPE CREEK GENERATING STATION

AND SALEM NUCLEAR GENERATING STATION, UNIT NOS. 1 AND 2

DOCKET NOS. 50-354, 50-272, AND 50-311

## 1.0 INTRODUCTION

By application dated July 14, 2010, as supplemented by letters dated September 28, 2010, April 1, 2011, June 6, 2011, and July 6, 2011 (References 1 through 5), PSEG Nuclear LLC (PSEG or the licensee) submitted license amendment requests for the Hope Creek Generating Station (HCGS) and Salem Nuclear Generating Station (Salem) Unit Nos. 1 and 2.

The proposed amendments would approve the Cyber Security Plan (CSP) and associated implementation schedule for HCGS and Salem Unit Nos. 1 and 2. In addition, the amendments would revise the existing license condition regarding physical protection in the each of the three facility operating licenses (FOLs) to require the licensee to fully implement and maintain in effect all provisions of the Nuclear Regulatory Commission (NRC or Commission)-approved CSP. The proposed amendment was submitted pursuant to Section 73.54 of Title 10 of the *Code of Federal Regulations* (10 CFR) which requires licensees currently licensed to operate a nuclear power plant under 10 CFR Part 50 to submit a CSP for NRC review and approval.

The supplements dated September 28, 2010, April 1, 2011, June 6, 2011, and July 6, 2011, provided additional information that clarified the application, did not expand the scope of the application as originally noticed, and did not change the NRC staff's original proposed no significant hazards consideration determination as published in the *Federal Register* (FR) on October 12, 2010 (75 FR 62606).

## 2.0 REGULATORY EVALUATION

### 2.1 General Requirements

Nuclear power plant licensees' physical protection programs must cornply with the performance objectives and requirements in 10 CFR 73.55, "Requirements for physical protection of licensed activities in nuclear power reactors against radiological sabotage."

As required by 10 CFR 73.55(a)(1), a licensee must implement the requirements of this section through its Commission-approved physical security plan, training and qualification plan, safeguards contingency plan, and CSP, referred to collectively as "security plans."

As stated in 10 CFR 73.54(b)(3), the Cyber Security Program is a component of the physical protection program. In accordance with 10 CFR 73.55(b)(8), licensees are required to establish, maintain, and implement a Cyber Security Program in accordance with 10 CFR 73.54.

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 6), the Commission 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 (RG) 5.71 and Nuclear Energy Institute (NEI) 08-09, Revision 6

RG 5.71, "Cyber Security Programs for Nuclear Facilities," (Reference 7) 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 CSP 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 contains information comparable to that found in Appendices A, B, and C of RG 5.71 as follows: (1) Appendix A of NEI 08-09, Revision 6 contains a cyber security plan template that is comparable to Appendix A of RG 5.71; (2) Appendix D of NEI 08-09, Revision 6 contains technical cyber security controls that are comparable to Appendix B of RG 5.71; and (3) 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 to NEI dated May 5, 2010 (Reference 8), that licensees may use the template in NEI 08-09, Revision 6 (Reference 9), 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 10), a definition for "cyber attack" to be used in submissions based on NEI 08-09, Revision 6. The licensee submitted a CSP for the HCGS and Salem Units 1 and 2 that was based on the template provided in NEI 08-09, Revision 6 and included a definition of cyber attack acceptable to the NRC staff in the deviation table within the original CSP submittal. Additionally, the licensee submitted a supplement to their CSP on April 1, 2011, to include information on SSCs in the BOP that, if compromised, could affect NPP 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 NRC staff reviewed the submitted CSP against the corresponding sections in RG 5.71.

## 3.0 TECHNICAL EVALUATION

The NRC staff performed a technical evaluation of the information provided by the licensee (i.e., References 1 through 5). The licensee's application dated July 14, 2010 (Reference 1), provided the Salem-Hope Creek CSP, an implementation schedule, proposed license changes and a discussion of deviations that PSEG has taken to the guidance in NEI 08-09, Revision 6. The licensee's letter dated June 6, 2011 (Reference 4) provided a revised CSP, a revised implementation schedule, and revised proposed license changes that superseded the corresponding information provided in Reference 1. The proposed license changes in Reference 4 were subsequently superseded by the information provided in the licensee's letter dated July 6, 2011 (Reference 5). The licensee's letter dated September 28, 2010 (Reference 2), stated that PSEG would provide a supplement to clarify the scope of SSCs included in the CSP. This information was subsequently provided by the licensee in its letter dated April 1, 2011 (Reference 3). The letter dated April 1, 2011, also provided information to clarify the proposed amendments in response to an NRC staff request for additional information.

The licensee's CSP, with the exceptions and deviations described below, 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. The staff reviewed the licensee's CSP against the requirements of 10 CFR 73.54 following the guidance contained in RG 5.71. The staff's evaluation of each section of the CSP is discussed below.

### 3.1 Scope and Purpose

The licensee's 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 licensee's CSP, as originally submitted, is comparable to the CSP in NEI-08-09, Revision 6. However, in its submittal dated April 1, 2011, the licensee 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 consistent with SRM-COMWCO-10-0001 (Reference 6), in which the Commission stated that the NRC's cyber security rule at 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 licensee 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 licensee 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 licensee's CSP states 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 licensee 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 licensee 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 licensee established adequate measures to define and address the purpose, scope, roles, responsibilities, management commitment, and coordination, and to facilitate 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 (CSAT)

The CSAT 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 included 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 licensee 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 states that the licensee 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 licensee 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 licensee's 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 licensee can implement security controls on a CDA, it 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 licensee 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 states 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 licensee 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 licensee established defense-in-depth strategies by implementing and documenting: (1) 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; (2) a physical security program, including physical barriers; (3) 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 (4) the technical controls described in Appendix D of NEI 08-09, Revision 6, which is comparable to Appendix B to RG 5.71.

The licensee modified the defense-in-depth strategy as outlined in the NEI and NRC templates. However, the final version of their CSP 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 above, 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 licensee 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 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, response, containment, eradication, and recovery activities comparable to Section 4.6 of NEI 08-09, Revision 6.

This section of the CSP submitted by the licensee 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 licensee describes the Cyber Security Contingency Plan that would include the response to events. The plan includes 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 licensee 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 licensee's 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: (1) awareness training; (2) technical training; and (3) specialized cyber security training.

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

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 licensee 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 policies and procedures.

The CSP also describes the licensee's 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 licensee 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 the 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. The CSIRT initiates in accordance with the Incident Response Plan and 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 describes that the licensee has 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 stated 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 guidance provided by industry to licensees did not fully comply with the requirements of 10 CFR 73.54.

In a letter to the NRC dated February 28, 2011 (Reference 11), NEI provided proposed text that supersedes, in entirety, the existing text in Section 4.13 of NEI 08-09, Revision 6. The proposed text 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. The proposed text states that 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. In a letter to NEI dated March 1, 2011 (Reference 12), the NRC staff stated that the staff has identified no issues with the language proposed by NEI's letter dated February 28, 2011. 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 its letter dated April 1, 2011 (Reference 3), the licensee responded to the records retention issue using the language proposed by NEI's letter dated February 28, 2011.

This section of the CSP submitted by the licensee is comparable to Regulatory Position C.5 and Appendix A, Section A.5 of RG 5.71 without deviation.

Based on the above, the NRC staff finds that the language the licensee proposes to adopt provides for adequate records retention and will support the licensee's ability to detect and respond to cyber attacks. Accordingly, the NRC staff concludes that the licensee's 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 to the NRC dated February 28, 2011 (Reference 13), NEI provided a template for licensees to use to submit their CSP implementation schedules. In a letter to NEI dated March 1, 2011 (Reference 14), the NRC staff stated that the staff has identified no issues with the CSP implementation schedule template proposed by NEI's letter dated February 28, 2011. The key intermediate milestones in the implementation schedule template 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.

In its letter dated June 6, 2011 (Reference 4), the licensee provided a revised implementation schedule using the NEI template. The NRC staff considers the implementation schedule in the June 6, 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 finds the Cyber Security Program implementation schedule is satisfactory.

Consistent with the discussion in the NRC's letter to Holders of Licenses for Operating Power Reactors dated May 9, 2011 (Reference 15), the following paragraph would be added to the license amendment authorization page upon approval of the respective amendments for HCGS and Salem Unit Nos. 1 and 2:

> This license amendment is effective as of the date of its issuance. The implementation of the Cyber Security Plan (CSP), including the key intermediate milestone dates and the full implementation date, shall be in accordance with the implementation schedule submitted by the licensee by letter dated June 6, 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.

3.23 Differences from NEI 08-09, Revision 6

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

- In Section 3.1, "Scope and Purpose," the licensee clarified the definition of important-to-safety functions, consistent with SRM-COMWCO-10-0001.

- In Section 3.21, "Document Control and Records Retention and Handling," the licensee clarified the definition of records and supporting documentation that will be retained to conform to the requirements of 10 CFR 73.54.

- In Section 3.22, "Implementation Schedule," the licensee submitted a revised implementation schedule, specifying the interim milestones and the final implementation date, including supporting rationale.

The NRC staff finds all of these deviations to be acceptable as discussed in the respective sections.

3.24 Revision to License Condition 2.E

In its letter dated July 6, 2011 (Reference 5), the licensee proposed to add a paragraph to existing License Condition 2.E in each of the three FOLs. This license condition currently requires the licensee to fully implement and maintain in effect all provisions of the Commission-approved physical security, training and qualification, and safeguards contingency plans. The new paragraph would add requirements associated with the CSP. Specifically, the new paragraph would read as follows:

> PSEG Nuclear LLC 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 Salem-Hope Creek CSP was approved by License Amendment No. [ ].

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

3.25 Technical Evaluation Conclusion

The NRC staff's review and evaluation of the licensee's CSP was conducted using the staff positions established in the relevant sections of RG 5.71. Based on the NRC staff's review, the NRC finds that the licensee 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 licensee's Cyber Security Program provides high assurance that digital computer and communication systems and networks associated with the following 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.

Based on the above technical evaluation, the NRC staff concludes that the proposed CSP is acceptable.

## 4.0 STATE CONSULTATION

In accordance with the Commission's regulations, the New Jersey State Official was notified of the proposed issuance of the amendments. The State official had no comments.

## 5.0 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 amendment involves no significant hazards consideration, and there has been no public comment on such finding (75 FR 62606, dated October 12, 2010). Also, the amendments relate to changes in recordkeeping, reporting, or administrative procedures or requirements and to safeguards matters and do not involve any significant construction impacts. Accordingly, the amendments meet the eligibility criteria for categorical exclusion set forth in 10 CFR 51.22(c)(9), 10 CFR 51.22(c)(10), and 10 CFR 51.22(c)(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.

## 6.0 CONCLUSION

The Commission has concluded, based on the considerations discussed above, that: (1) there is reasonable assurance that the health and safety of the public will not be endangered by operation in the proposed manner, (2) such activities will be conducted in compliance with the Commission's regulations, and (3) the issuance of the amendments will not be inimical to the common defense and security or to the health and safety of the public.

## 7.0 REFERENCES

1. PSEG letter (LR-N10-0235) to NRC dated July 14, 2010, "Request for Approval of Salem-Hope Creek Cyber Security Plan" (submittal includes publicly available letter (Agencywide Documents Access and Management System (ADAMS) Accession No. ML102080586) and non-publicly available security-related enclosures (ADAMS Accession No. ML102080587)).

2. PSEG letter (LR-N10-0354) to NRC dated September 28, 2010, "Notification Letter Designating Salem and Hope Creek Generating Stations Balance of Plant Systems within Cyber Security Rule," (ADAMS Accession No. ML102810304).

3. PSEG letter (LR-N11-0079) to NRC dated April 1, 2011, "Response to Request for Additional Information for Approval of Salem-Hope Creek Cyber Security Plan" (submittal includes publicly available letter (ADAMS Accession No. ML110950185) and non-publicly available security-related enclosures (ADAMS Accession No. ML110940009)).

4. PSEG letter (LR-N11-0159) to NRC dated June 6, 2011, "Request for Approval of Salem-Hope Creek Cyber Security Plan" (submittal includes publicly available letter (ADAMS Accession No. ML111791803) and non-publicly available security-related enclosures (ADAMS Accession No. ML111580606)).

5. PSEG letter (LR-N11-0208) to NRC dated July 6, 2011, "Revised License Condition - Salem-Hope Creek Cyber Security Plan Supplement Submittal" (ADAMS Accession No. ML111880126).

6. NRC Staff Requirements Memorandum SRM-COMWCO-10-0001, "Regulation of Cyber Security at Nuclear Power Plants," dated October 21, 2010 (ADAMS Accession No. ML102940009).

7. Regulatory Guide 5.71, RG 5.71, "Cyber Security Programs for Nuclear Facilities," dated January 2010 (ADAMS Accession No. ML090340159).

8. NRC letter to NEI dated May 5, 2010, "Nuclear Energy Institute 08-09, Cyber Security Plan Template, Rev. 6" (ADAMS Accession No. ML101190371).

9. Nuclear Energy Institute NEI 08-09, Revision 6, "Cyber Security Plan for Nuclear Power Reactors," dated April 2010 (ADAMS Package Accession No. ML101180402).

10. NRC letter to NEI dated June 7, 2010, "Nuclear Energy Institute 08-09, Cyber Security Plan Template, Rev. 6" (ADAMS Accession No. ML101550052).

11. NEI letter to NRC dated February 28, 2011, "Clarification to NEI 08-09, Revision 6 Regarding Records Retention" (ADAMS Package Accession No. ML110600203).

12. NRC letter to NEI dated March 1, 2011, "Cyber Security Plan Generic Request for Additional Information on Records Retention" (ADAMS Accession No. ML110490337).

13. NEI letter to NRC dated February 28, 2011, "Template for the Cyber Security Plan Implementation Schedule" (ADAMS Package Accession No. ML110600206).

14. NRC letter to NEI dated March 1, 2011, "Template for Cyber Security Plan Implementation Schedule" (ADAMS Accession No. ML110070348).

15. NRC letter to Holders of Licenses for Operating Power Reactors dated May 9, 2011, "Cyber Security Plan Implementation Schedule," (ADAMS Accession No. ML110980538).

Principal Contributor: R. Harren

Date: July 28, 2011

A copy of our safety evaluation is also enclosed. Notice of Issuance will be included in the Commission's biweekly *Federal Register* notice.

Sincerely,

***/ra/***

Richard B. Ennis, Senior Project Manager
Plant Licensing Branch I-2
Division of Operating Reactor Licensing
Office of Nuclear Reactor Regulation

Docket Nos. 50-354, 50-272, and 50-311

Enclosures:
1. Amendment No. 189 to Renewed License No. NPF-57
2. Amendment No. 300 to Renewed License No. DPR-70
3. Amendment No. 283 to Renewed License No. DPR-75
4. Safety Evaluation

cc w/encls: Distribution via ListServ

DISTRIBUTION

PUBLIC
RidsNrrDorlLpl1-2 Resource
RidsNrrLAABaxter Resource
RidsRgn1MailCenter Resource
RHarren, NSIR
LPL 1-2 R/F
RidsAcrsAcnw_MailCTR Resource
RidsNrrDirsItsb Resource
RidsNrrDorlDpr Resource
RidsOgcRp Resource
GHill, OIS
RidsNrrPMSalem Resource
PPederson, NSIR

ADAMS Accession No: ML111861560 *SE dated 7/1/11

| OFFICE | LPL1-2/PM | LPL1-1/LA | NSIR/DSP/ISCPB/BC* | OGC | LPL1-2/BC |
|---|---|---|---|---|---|
| NAME | REnnis | SLittle | CErlanger | BMizuno | HChernoff |
| DATE | 7/28/11 | 7/18/11 | 7/1/11 | 7/26/11 | 7/28/11 |

OFFICIAL RECORD COPY