



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

August 23, 2011

Mr. Paul Freeman  
Site Vice President  
c/o Michael O'Keefe  
Seabrook Station  
NextEra Energy Seabrook, LLC  
P.O. Box 300  
Seabrook, NH 03874

SUBJECT: SEABROOK STATION, UNIT NO. 1 - ISSUANCE OF AMENDMENT RE:  
APPROVAL OF CYBER SECURITY PLAN (TAC NO. ME4453)

Dear Mr. Freeman:

The Commission has issued the enclosed Amendment No. 127 to Facility Operating License (FOL) No. NPF-86 for the Seabrook Station, Unit No. 1 (Seabrook). This amendment consists of changes to the License in response to your application dated July 26, 2010, as supplemented by letters dated September 28, 2010, March 31, 2011, June 23, and August 4, 2011.

The amendment approves the Cyber Security Plan (CSP) and associated implementation schedule for Seabrook. In addition, the amendment revises the existing license condition regarding physical protection in the FOL to require full implementation and maintenance of all provisions of the Nuclear Regulatory Commission (NRC)-approved CSP. The amendment was submitted pursuant to Section 73.54 of Title 10 of the *Code of Federal Regulations*.

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

Sincerely,

A handwritten signature in black ink, appearing to read "G. Edward Miller".

G. Edward Miller, Project Manager  
Plant Licensing Branch I-2  
Division of Operating Reactor Licensing  
Office of Nuclear Reactor Regulation

Docket No. 50-443

Enclosures:

1. Amendment No. 127 to NPF-86
2. Safety Evaluation

cc w/encls: Distribution via Listserv



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

NEXTERA ENERGY SEABROOK, LLC, ET AL.\*

DOCKET NO. 50-443

SEABROOK STATION, UNIT NO. 1

AMENDMENT TO FACILITY OPERATING LICENSE

Amendment No. 127

License No. NPF-86

1. The Nuclear Regulatory Commission (the Commission) has found that:
  - A. The application for amendment filed by NextEra Energy Seabrook, LLC, et al., (the licensee) dated July 26, 2010, as supplemented by letters dated September 28, 2010, March 31, June 23, and August 4, 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;
  - 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.

---

\*NextEra Energy Seabrook, LLC is authorized to act as agent for the: Hudson Light & Power Department, Massachusetts Municipal Wholesale Electric Company, and Taunton Municipal Light Plant and has exclusive responsibility and control over the physical construction, operation and maintenance of the facility.

2. Paragraph 2.E of Facility Operating License No. NPF-86 is hereby amended to add the following text:

NextEra Energy Seabrook, 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 NextEra Energy Seabrook, LLC CSP was approved by License Amendment No. 127 .

3. This license amendment is effective as of its date of issuance. The implementation of the CSP, including key intermediate milestone dates and the full implementation date, shall be in accordance with the implementation schedule submitted by the licensee by letter dated March 31, 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

A handwritten signature in black ink, appearing to read "H. Chernoff", with a small "for" written below it.

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: August 23, 2011

ATTACHMENT TO LICENSE AMENDMENT NO. 127

FACILITY OPERATING LICENSE NO. NPF-86

DOCKET NO. 50-443

Replace the following page of Facility Operating License No. NPF-86 with the attached revised page. The revised page is identified by amendment number and contains a marginal line indicating the area of change.

Remove  
6

Insert  
6

E. Physical 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 provision 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 combined set of plans<sup>1</sup>, submitted by letter dated September 23, 2004, and supplemented by letters dated October 15, October 22, and October 29, 2004, and May 18, 2006, is entitled: "Florida Power and Light & FPL Energy Seabrook Physical Security Plan, Training and Qualification Plan and Safeguards Contingency Plan." The set contains Safeguards Information protected under 10 CFR 73.21. NextEra Energy Seabrook, 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 NextEra Energy Seabrook, LLC CSP was approved by License Amendment No. 127.

F. Fire Protection

NextEra Energy Seabrook, LLC, shall implement and maintain in effect all provisions of the approved fire protection program as described in the Final Safety Analysis Report, the Fire Protection Program Report, and the Fire Protection of Safe Shutdown Capability report for the facility, as supplemented and amended, and as approved in the Safety Evaluation Report, dated March 1983; Supplement 4, dated May 1986; Supplement 5, dated July 1986; Supplement 6, dated October 1986; Supplement 7, dated October 1987; and Supplement 8, dated May 1989 subject to the following provisions: NextEra Energy Seabrook, LLC, 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 shutdown in the event of a fire.

G. DELETED

H. Financial Protection

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.

I. DELETED

---

<sup>1</sup>The Training and Qualification Plan and Safeguards Contingency Plan are Appendices to the Security Plan.



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

SAFETY EVALUATION BY THE OFFICE OF NUCLEAR REACTOR REGULATION

RELATED TO AMENDMENT NO. 127

TO FACILITY OPERATING LICENSE NO. NPF-86

SEABROOK STATION, UNIT NO. 1

DOCKET NO. 50-443

1.0 INTRODUCTION

By letter dated July 26, 2010,<sup>1</sup> as supplemented by letters dated September 28, 2010, March 31, June 23, and August 4, 2011,<sup>2</sup> NextEra Energy Seabrook, LLC. submitted a license amendment request. Included in that license amendment request was a request for approval of the licensee's Cyber Security Plan (CSP) and Implementation Schedule for the Seabrook Station, Unit 1 as required by Title 10 of the *Code of Federal Regulations* (10 CFR) 73.54. On March 31, 2011, the licensee supplemented their CSP, to address: 1) scope of systems in response to the October 21, 2010, Commission decision (Reference 5); 2) records retention; and 3) implementation schedule. The March 31, 2011, supplement included a revised version of the CSP incorporating all of the changes and/or additional information.

The September 28, 2010, March 31, June 23, and August 4, 2011, supplements contained clarifying information and did not change the U.S. Nuclear Regulatory Commission (NRC) staff's initial proposed finding of no significant hazards consideration as published in the *Federal Register* on May 10, 2011 (76 FR 27097).

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

---

<sup>1</sup> Agencywide Documents Access and Management System (ADAMS) Accession No. ML102140179

<sup>2</sup> ADAMS Accession Nos. ML102780426, ML110950667, ML11180A058, and ML11222A019, respectively

systems, services, or data; or provide an adverse impact to the operations of systems, networks, and associated equipment.

In the Staff Requirements Memorandum (SRM)-COMWCO-10-0001, "Regulation of Cyber Security of Nuclear Power Plants," dated October 21, 2010 (Reference 1), 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 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 Nuclear Energy Institute (NEI) 08-09, Revision 6

NRC Regulatory Guide (RG) 5.71, "Cyber Security Programs for Nuclear Facilities," (Reference 2) 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.

In its letter to NEI dated May 5, 2010 (Reference 3), the NRC stated that the licensee may use the template in NEI 08-09, Revision 6 (Reference 4), 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 5), a definition for "cyber attack" to be used in submissions based on NEI 08-09, Revision 6. The licensee submitted a CSP for the Seabrook Station, Unit 1 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 "NEI 08-09 Clarifications" portion of Section 3.0, "Technical Evaluation" of Enclosure 1 to the CSP, "Evaluation of Proposed Changes." Additionally, the licensee submitted a supplement to its CSP on March 31, 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 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 licensee's submittal. The licensee's submittal, with the exceptions described in Section 4.0 of this safety evaluation, 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 NRC staff reviewed the licensee's submittal against the requirements of 10 CFR 73.54 following the guidance contained in RG 5.71. The staff's evaluation of each section of their submittal 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 March 31, 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 in response to and consistent with SRM-COMWCO-10-0001, 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).

On June 23, 2011, the licensee withdrew a clarification statement to NEI 08-09, Revision 6 regarding Emergency Preparedness functions within the scope of the CSP as provided in the July 26, 2010, licensee amendment request, Enclosure 1, Section 3.0. As a result, the licensee has indicated that no clarifications or deviation from NEI 08-09, Revision 6 is required.

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 concludes 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 concludes 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 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 CSP submitted by the licensee 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 concludes 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 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 concludes 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 Cyber Security Assessment Team (CSAT) responsibilities include conducting the cyber security assessment, documenting key findings during the assessment, and evaluating assumptions and conclusions about cyber security threats. The CSP submitted by the licensee 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 CSP submitted by the licensee 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 CSP submitted by the licensee 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 concludes that the CSP adequately establishes the requirements, roles, and responsibilities of the CSAT.

### 3.5 Identification of CDAs

The CSP submitted by the licensee 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 concludes that the CSP adequately describes the process to identify CDAs.

### 3.6 Examination of Cyber Security Practices

The CSP submitted by the licensee 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 concludes that the CSP adequately describes the examination of cyber security practices.

### 3.7 Tabletop Reviews and Validation Testing

The CSP submitted by the licensee 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 CSP submitted by the licensee 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 CSP submitted by the licensee 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 concludes 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 CSP submitted by the licensee 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 concludes that the CSP adequately describes review of the CSP as a component of the physical security program.

### 3.10 Cyber Security Controls

The CSP submitted by the licensee 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 licensee is comparable to Appendix A, Section A.3.1.6 in RG 5.71 without deviation.

Based on the above, the NRC staff concludes 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: 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 licensee stated in the CSP that the boundary between Level 3 and Level 4 is implemented by one or more deterministic devices, while information flows between Level 3 and Level 2 are restricted through the use of a firewall and network-based intrusion detection system and/or prevention system. The NRC staff finds this defense-in-depth protective strategy to be acceptable based on the statement in the CSP that the firewall will implement the Information Flow Enforcement cyber security control in NEI 08-09, Revision 6, Appendix D, Section 1.4 and the rule set characteristics for non-deterministic information flow enforcement described in the Defense-in-Depth cyber security control in NEI 08-09, Revision 6, Appendix E, Section 6.

This section of the CSP submitted by the licensee is comparable to Regulatory Position C.3.2 and Appendix A, Section A.3.1.5 in RG 5.71.

Based on the above, the NRC staff concludes that the CSP adequately describes implementation of defense-in-depth protective strategies.

### 3.12 Ongoing Monitoring and Assessment

The CSP submitted by the licensee 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 concludes that the CSP adequately describes ongoing monitoring and assessment.

### 3.13 Modification of Digital Assets

The CSP submitted by the licensee 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 concludes that the CSP adequately describes modification of digital assets.

### 3.14 Attack Mitigation and Incident Response

The CSP submitted by the licensee 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 concludes that the CSP adequately describes attack mitigation and incident response.

### 3.15 Cyber Security Contingency Plan

The CSP submitted by the licensee 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 concludes that the CSP adequately describes the cyber security contingency plan.

### 3.16 Cyber Security Training and Awareness

The CSP submitted by the licensee 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: awareness training, technical training, and specialized cyber security training.

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

### 3.17 Evaluate and Manage Cyber Risk

The CSP submitted by the licensee 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 concludes 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 concludes that the CSP adequately describes cyber security policies and implementing procedures.

### 3.19 Roles and Responsibilities

The CSP submitted by the licensee 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 concludes that the CSP adequately describes cyber security roles and responsibilities.

### 3.20 Cyber Security Program Review

The CSP submitted by the licensee 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 concludes that the CSP adequately describes Cyber Security Program review.

### 3.21 Document Control and Records Retention and Handling

The CSP submitted by the licensee 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 dated February 28, 2011 (ADAMS Accession No. ML110600204), NEI sent to the NRC proposed language for licensees' use to respond to the generic records retention issue, to which the NRC had no technical objection (Reference: Letter from NRC dated March 1, 2011, ADAMS Accession No. ML110490337). The proposed language clarified the requirement by providing 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 a letter dated March 31, 2011 (ADAMS Accession No. ML110950667), the licensee responded to the records retention issue using the language proposed by NEI in its 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 has proposed to adopt provides for adequate records retention and will support the licensee's 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 licensee's CSP adequately describes cyber security document control and records retention and handling.

### 3.22 Implementation Schedule

The CSP submitted by the licensee provides a proposed implementation schedule for the Cyber Security Program. In a letter dated February 28, 2011 (ADAMS Accession No. ML110600206), 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: Letter from NRC dated March 1, 2011, ADAMS Accession No. ML110070348). 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.

By letter dated March 31, 2011 (ADAMS Accession No. ML110950667), the licensee provided a revised implementation schedule using the NEI template. The NRC staff considers this March 31, 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 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 (ADAMS Accession No. ML110980538), the following paragraph would be added to the license amendment authorization page upon approval of the amendment:

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 March 31, 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 License Condition

In its letter dated August 4, 2011, the licensee proposed to add a paragraph to existing License Condition 2.E of the FOL. 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:

NextEra Energy Seabrook, 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 NextEra Energy Seabrook, LLC CSP was approved by License Amendment No.

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

## 4.0 DIFFERENCES FROM NEI 08-09, REVISION 6

In addition to Section 3.0, "NEI 08-09 Clarifications" found in Enclosure 1 to the CSP, 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. The licensee amendment request letter included a clarification to the NEI 08-09, Revision 6 that narrowed the scope of Emergency Preparedness systems within the scope of the Rule; after discussions with NRC staff, the licensee retracted this clarification. It is important to note that this is no longer different than NEI 08-09, Revision 6; the original difference is mentioned in this section for completeness of record.
- 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 concludes all of these deviations to be acceptable as discussed in the respective sections.

## 5.0 STATE CONSULTATION

In accordance with the Commission's regulations, the New Hampshire and Massachusetts State officials were notified of the proposed issuance of the amendment. The State officials provided no comments.

## 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 May 10, 2011 (76 FR 27097). 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 51.21(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 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 concludes 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 communications 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.

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) there is reasonable assurance that such activities will be conducted in compliance with the Commission's regulations; and (3) the issuance of the amendment will not be inimical to the common defense and security or to the health and safety of the public.

## 8.0 REFERENCES

1. Memorandum from Annette Vietti-Cook to R.W. Borchardt, U.S. Nuclear Regulatory Commission, "Staff Requirements – COMWCO-10-000 – Regulation of Cyber Security at Nuclear Power Plants," dated October 21, 2010 (ADAMS Accession No. ML102940009).
2. Regulatory Guide 5.71, "Cyber Security Programs for Nuclear Facilities," U.S. Nuclear Regulatory Commission, Washington, DC, January 2010. (ADAMS Accession No. ML090340159).
3. Letter from Richard Correia, U.S. Nuclear Regulatory Commission, to Jack Roe, Nuclear Energy Institute, "Nuclear Energy Institute 08-09, 'Cyber Security Plan Template, Revision 6,'" May 5, 2010. (ADAMS Accession No. ML101190371).
4. Letter from Jack Roe, Nuclear Energy Institute, to Scott Morris, U.S. Nuclear Regulatory Commission, "NEI 08-09, Revision 6, 'Cyber Security Plan for Nuclear Power Reactors; April 2010,'" April 28, 2010. (ADAMS Accession No. ML101180434).
5. Letter from Richard Correia, U.S. Nuclear Regulatory Commission, to Christopher E. Earls, Nuclear Energy Institute, "Nuclear Energy Institute 08-09, 'Cyber Security Plan Template; Rev. 6'", dated June 7, 2010 (ADAMS Accession No. ML101550052).

Principal Contributor: M. Coflin

Date: August 23, 2011

August 23, 2011

Mr. Paul Freeman  
Site Vice President  
c/o Michael O'Keefe  
Seabrook Station  
NextEra Energy Seabrook, LLC  
P.O. Box 300  
Seabrook, NH 03874

SUBJECT: SEABROOK STATION, UNIT NO. 1 - ISSUANCE OF AMENDMENT RE:  
APPROVAL OF CYBER SECURITY PLAN (TAC NO. ME4453)

Dear Mr. Freeman:

The Commission has issued the enclosed Amendment No. 127 to Facility Operating License (FOL) No. NPF-86 for the Seabrook Station, Unit No. 1 (Seabrook). This amendment consists of changes to the License in response to your application dated July 26, 2010, as supplemented by letters dated September 28, 2010, March 31, 2011, June 23, and August 4, 2011.

The amendment approves the Cyber Security Plan (CSP) and associated implementation schedule for Seabrook. In addition, the amendment revises the existing license condition regarding physical protection in the FOL to require full implementation and maintenance of all provisions of the Nuclear Regulatory Commission (NRC)-approved CSP. The amendment was submitted pursuant to Section 73.54 of Title 10 of the *Code of Federal Regulations*.

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/

G. Edward Miller, Project Manager  
Plant Licensing Branch I-2  
Division of Operating Reactor Licensing  
Office of Nuclear Reactor Regulation

Docket No. 50-443

Enclosures:

1. Amendment No. 127 to NPF-86
2. Safety Evaluation

cc w/encls: Distribution via Listserv

DISTRIBUTION:

PUBLIC	LPLI-2 R/F	RidsAcrsAcnw_MailCTR Resource
RidsNrrDorIDpr Resource	RidsNrrDorLp1-2 Resource	RidsRgn1MailCenter Resource
GHill, OIS	RidsNrrPMSeabrook Resource	RidsNrrLAABaxter Resource
RidsOgcRp Resource	PPederson, NSIR	RHarren, NSIR
RidsNrrDirsltsb Resource		

ADAMS Accession No.: ML112070048

\*Via e-mail (ML111920051)

OFFICE	LPL1-2/PM	LPL1-2/LA	NSIR/DSP/ISCPB/BC	OGC	LPL1-2/BC
NAME	GEMiller	ABaxter (via e-mail)	CErlanger*	BHarris	HChernoff (REnnis for)
DATE	8/23/11	8/23/11	7/9/11	8/1/11	8/23/11

Official Record Copy