SECURITY-RELATED INFORMATION
~~WITHHOLD FROM PUBLIC DISCLOSURE UNDER 10 CFR 2.390~~

NEXTera ENERGY POINT BEACH

March 31, 2011

NRC 2011-0033
10 CFR 50.90

U.S. Nuclear Regulatory Commission
ATTN: Document Control Desk
Washington, DC 20555

Point Beach Nuclear Plant, Units 1 and 2
Dockets 50-266 and 50-301
Renewed License Nos. DPR-24 and DPR-27

Supplement to License Amendment Request 263,
Response to Request for Additional Information

References: (1) NextEra Energy Point Beach, LLC letter to NRC, dated July 8, 2010, License Amendment Request 263, Request for Approval of the Point Beach Plant Revised Cyber Security Plan (ML101900312)

(2) NRC letter to NextEra Energy Point Beach, LLC, dated March 7, 2011, Point Beach Nuclear Plant, Units 1 and 2 - Request for Additional Information Regarding License Amendment Request for Approval of Revised Cyber Security Plan (TAC Nos. ME4248 and ME4249) (ML110620514)

In Reference (1) and in accordance with the provisions of 10 CFR 50.4 and 50.90, NextEra Energy Point Beach, LLC (NextEra) submitted a request for amendment to the Renewed Facility Operating Licenses for Point Beach Nuclear Plant (PBNP). This proposed amendment requested NRC approval of the NextEra Cyber Security Plan (CSP), provided an implementation schedule and revised License Condition D of the Renewed Facility Operating Licenses to require PBNP to fully implement and maintain in effect all provisions of the Commission-approved CSP. NextEra has determined that in response to Reference (2), a revision to Sections 2.1 and 4.13 of the CSP is required.

Via Reference (2), NRC staff determined that additional information was required to complete their review of the proposed amendment. Enclosure 1 provides the NextEra response to the NRC request for additional information.

Enclosure 2 provides an evaluation of the proposed change. Attachment 1 of Enclosure 2 provides the existing Renewed Facility Operating License pages marked up to show the proposed change.

Enclosure 4 to this letter contains sensitive information.
Withhold from public disclosure under 10 CFR 2.390.
Upon removal of Enclosure 4, this letter is uncontrolled.

S001A
NRR

Enclosure 3 provides a copy of the revised PBNP CSP implementation schedule.

Enclosure 4 provides a copy of the PBNP CSP containing revisions to Sections 2.1 and 4.13, in response to the request for additional information (Reference 2). NextEra requests that Enclosure 4, which contains sensitive information, be withheld from public disclosure in accordance with 10 CFR 2.390(d)(1).

The PBNP Plant Operations Review Committee has reviewed the proposed supplement to the license amendment request.

This letter contains no new Regulatory Commitments and no revisions to existing Regulatory Commitments.

In accordance with 10 CFR 50.91, a copy of this letter is being provided to the designated Wisconsin Official.

If you have any questions or require additional information, please contact James Costedio, Licensing Manager, at 920/755-7427

I declare under penalty of perjury that the foregoing is true and correct.
Executed on March 31, 2011.

Very truly yours,

NextEra Energy Point Beach, LLC

Larry Meyer
Site Vice President

Enclosures

cc: Administrator, Region III, USNRC
Project Manager, Point Beach Nuclear Plant, USNRC
Resident Inspector, Point Beach Nuclear Plant, USNRC
PSCW

Enclosure 4 to this letter contains sensitive information.
Withhold from public disclosure under 10 CFR 2.390.
Upon removal of Enclosure 4, this letter is uncontrolled.

ENCLOSURE 1

NEXTERA ENERGY POINT BEACH, LLC
POINT BEACH NUCLEAR PLANT, UNITS 1 AND 2

SUPPLEMENT TO LICENSE AMENDMENT REQUEST 263,
RESPONSE TO REQUEST FOR ADDITIONAL INFORMATION

RESPONSE TO REQUEST FOR ADDITIONAL INFORMATION

Via Reference (1), NRC staff determined that additional information was required to complete their review of License Amendment Request (LAR) 263, Cyber Security Plan (CSP). The following is the NextEra Energy Point Beach, LLC (NextEra) response to the request.

RAI 1: Records Retention

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

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

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

NextEra Response

NextEra is submitting a revised Cyber Security Plan (CSP), provided in Enclosure 4, that incorporates language changes into Section 4.13 consistent with the language that the Nuclear Energy Institute (NEI) proposed to the NRC (ML110600204). NRC staff concurred with the proposed language (ML110490337).

RAI 2: Implementation Schedule

The regulation at 10 CFR 73.54, "Protection of digital computer and communication systems and networks," requires licensees to submit a CSP that satisfies the requirements of this section for Commission review and approval. Furthermore, each submittal must include a proposed implementation schedule and the implementation of the licensee's cyber security program must be consistent with the approved schedule. Paragraph 73.54(a) of 10 CFR requires licensees to provide high assurance that digital computer and communication systems and networks are adequately protected against cyber attacks, up to and including the design-basis threat (DBT).

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

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

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

NextEra Response

NextEra is submitting a revised CSP implementation schedule consistent with the template NEI provided to the NRC (ML110600211), which the NRC subsequently concurred with (ML110070348), and is provided in Enclosure 3.

RAI 3: Scope of Systems

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

Subsequent to the issuance of the cyber security rule, the NRC stated that 10 CFR 73.54 should be interpreted to include structures, systems, and components (SSCs) in the balance of plant (BOP) that have a nexus to radiological health and safety (ADAMS Accession No. ML 103490344, dated November 19, 2010). The SSCs in the BOP are those that could directly or indirectly affect reactivity of a nuclear power plant and could result in an unplanned reactor shutdown or transient and are, therefore, within the scope of important-to-safety functions described in 10 CFR 73.54{a)(1). Furthermore, the NRC issued a letter to NEI dated January 5, 2011 (ADAMS Accession No. ML 103550480), that provided licensees additional guidance on one acceptable approach to comply with the Commission's policy determination.

Explain how the scoping of systems provided by the site CSP meets the requirements of 10 CFR 73.54 and the additional guidance provided by the NRC.

NextEra Response

NextEra is submitting a revised CSP that incorporates the language changes into Section 2.1, consistent with the approach provided by the NRC (ML103550480). The revised CSP is provided as Enclosure 4.

References

(1) NRC letter to NextEra Energy Point Beach, LLC, dated March 7, 2011, Point Beach Nuclear Plant, Units 1 and 2 - Request for Additional Information Regarding License Amendment Request for Approval of Revised Cyber Security Plan (TAC Nos. ME4248 and ME4249) (ML110620514)

ENCLOSURE 2

NEXTERA ENERGY POINT BEACH, LLC
POINT BEACH NUCLEAR PLANT, UNITS 1 AND 2

SUPPLEMENT TO LICENSE AMENDMENT REQUEST 263,
RESPONSE TO REQUEST FOR ADDITIONAL INFORMATION

EVALUATION OF PROPOSED CHANGE

ATTACHMENT

Attachment 1 - Marked up Renewed Facility Operating License pages

5 pages follow

1.0 SUMMARY DESCRIPTION

In Reference 1, NextEra Energy Point Beach, LLC (NextEra) submitted a request for amendment to the Renewed Facility Operating Licenses, DPR-24 and DPR-27, for Point Beach Nuclear Plant (PBNP) Units 1 and 2, respectively. This proposed amendment requested NRC approval of the PBNP Security Plan, provided an implementation schedule, and added a sentence to the existing Renewed Facility Operating Licenses physical protection license condition to require NextEra to fully implement and maintain in effect all provisions of the Commission approved Cyber Security Plan. It has since been determined that a revision to Section 2.1, Scope and Purpose, and Section 4.13, Document Control And Records Retention And Handling, of the submitted Plan is required.

The change to Section 2.1 of the PBNP Cyber Security Plan clarifies the balance of plant structures, systems and components that are included in the scope of the cyber security program. This change also requires revision to the Evaluation of Proposed Change, and the Renewed Facility Operating Licenses pages submitted in Reference 1.

The change to Section 4.13 of the PBNP Cyber Security Plan clarifies the type of documentation that will be retained, and the length of time in which the documentation will be retained, in accordance with 10 CFR 73.554(h). This change also requires revision to the Evaluation of Proposed Change, and the Renewed Facility Operating Licenses pages submitted in Reference 1.

2.0 DETAILED DESCRIPTION

This supplement revises the proposed LAR (Reference 1) that included three parts: the proposed Plan, an Implementation Schedule, and a proposed sentence to be added to the existing Renewed Facility Operating Licenses Physical Protection license condition to require NextEra to fully implement and maintain in effect all provisions of the Commission approved Cyber Security Plan as required by 10 CFR 73.54. *Federal Register* notice 74 FR 13926 issued the final rule that amended 10 CFR Part 73. The regulations in 10 CFR 73.54, "Protection of digital computer and communication systems and networks," establish the requirements for a cyber security program. This regulation specifically requires each licensee currently licensed to operate a nuclear power plant under Part 50 of this chapter to submit a cyber security plan that satisfies the requirements of the Rule. Each submittal must include a proposed implementation schedule and implementation of the licensee's cyber security program must be consistent with the approved schedule. The background for this application is addressed by the NRC Notice of Availability published on March 27, 2009, 74 FR 13926 (Reference 2).

3.0 TECHNICAL EVALUATION

Federal Register notice 74 FR 13926 issued the final rule that amended 10 CFR 73. Cyber security requirements are codified as new 10 CFR 73.54 and are designed to provide high assurance that digital computer and communication systems and networks are adequately protected against cyber attacks up to and including the design basis threat established by 10 CFR 73.1(a)(1)(v). These requirements are substantial improvements upon the requirements imposed by EA-02-026 (Reference 2).

This supplement includes the proposed change to the existing Renewed Facility Operating Licenses condition for "Physical Protection" (Attachment 1), as well as the revised proposed Plan (Enclosure 4) that conforms to the template provided in NEI 08-09 Revision 6, with the following exceptions:

Definition of Cyber Attack

In lieu of the use of the definition of "cyber attack" in NEI 08-09, Revision 6, the definition of "cyber attack" contained in NEI letter dated June 2, 2010, and as accepted by the Commission via letter dated June 7, 2010, will be used.

Emergency Preparedness

10 CFR 73.54 requires protecting digital computer and communication systems and networks associated with emergency preparedness (EP) functions, including offsite communications. The EP functions within the scope of the Plan are those functions which support implementation of the Risk Significant Planning Standards* (RSPSs) as defined in NRC Inspection Manual Chapter 0609, Appendix B. The RSPSs are the subset of EP Planning Standards, defined in 10 CFR 50.47(b), which play the greatest role in protecting public health and safety. In terms of importance, this approach aligns the selected EP functions with other system functions, which are "Safety-Related" or "Important-to-Safety."

10 CFR 73.56(b)(ii) requires that any individual whose duties and responsibilities permit the individual to take actions by electronic means, either on site or remotely, that could adversely impact the licensee's emergency preparedness be subject to an access authorization program. However, some systems, or portions of systems, that perform an RSPS-related EP function may be located in offsite locations not under the control of the licensee and/or not staffed by licensee personnel. Similarly, there may be system components that are normally installed, modified, or maintained by non-licensee personnel (e.g., a telecommunications company technician, employee of a State agency, etc.).

Therefore, the systems, and portions of systems, to be protected from cyber attack in accordance with 10 CFR 73.54(a)(1)(iii) must;

1. Perform a RSPS-related EP function, and
2. Be within the licensee's complete custody and control.

* The RSPSs are 10 CFR 50.47(b)(4), (5), (9), and (10), including the related sections of Appendix E to 10 CFR Part 50. 10 CFR 50.47(b)(10) has two aspects that are of differing risk significance. Only the portion dealing with the development of protective action recommendations (PARs) is integral to protection of public health and safety and is considered to be an RSPS.

Senior Nuclear Management

Senior nuclear management is defined as the Vice President accountable for nuclear plant security. The NEI 08-09 template defines this position as accountable for nuclear plant operations. The position of Vice President accountable for nuclear plant security better reflects the duties and responsibilities of the PBNP Cyber Security Plan.

Balance of Plant Systems within Scope

The following paragraph is being added to Section 2.1, Scope and Purpose, of the Plan to clarify the balance of plant structures, systems, and components that are included in the scope of the cyber security program: "Within the scope of NRC's cyber security rule at Title 10 of the Code of Federal Regulations (10 CFR) 73.54, systems or equipment that perform important to safety functions include structures, systems, and components (SSCs) in the balance of plant (BOP) that could directly or indirectly affect reactivity at a nuclear power plant and could result in an unplanned reactor shutdown or transient. Additionally, these SSCs are under the licensee's control and include electrical distribution equipment out to the first inter-tie with the offsite distribution system."

Document Control and Records Retention and Handling

Section 4.13, Document Control And Records Retention And Handling, is being revised to provide examples of records or supporting technical documentation that are retained as a record until the Commission terminates the license for which the records are developed and to specify that superseded portions of these records are retained for three years unless otherwise specified by the Commission in accordance with the requirements of 10 CFR 73.54(h).

4.0 REGULATORY EVALUATION

4.1 Applicable Regulatory Requirements/Criteria

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

4.2 Significant Hazards Consideration

NextEra has evaluated whether or not a significant hazards consideration is involved with the proposed amendment by focusing on the three standards set forth in 10 CFR 50.92, "Issuance of Amendment," as discussed below:

1. Does the proposed amendment involve a significant increase in the probability or consequences of an accident previously evaluated?

   Response: No.

   The proposed amendment incorporates a new requirement in the Renewed Facility Operating License to implement and maintain a Cyber Security Plan as part of the facility's overall program for physical protection. Inclusion of the Cyber Security Plan in the Renewed Facility Operating License itself does not involve any modifications to the safety-related structures, systems, or components (SSCs). Rather, the Cyber Security Plan describes how the requirements of 10 CFR 73.54 are to be implemented to identify, evaluate, and mitigate cyber attacks up to and including the design basis cyber attack threat, thereby achieving high assurance that the facility's digital computer and communications systems and networks are protected from cyber attacks. The Cyber Security Plan will not alter previously evaluated Final Safety Analysis Report (FSAR) design basis accident analysis assumptions, add any accident initiators, or affect the function of the plant safety-related SSCs as to how they are operated, maintained, modified, tested, or inspected.

Therefore, the proposed amendment does not involve a significant increase in the probability or consequences of an accident previously evaluated.

2. Does the proposed amendment create the possibility of a new or different kind of accident from any accident previously evaluated?

   Response: No.

   This proposed amendment provides assurance that safety-related SSCs are protected from cyber attacks. Implementation of 10 CFR 73.54 and the inclusion of a plan in the Renewed Facility Operating License do not result in the need of any new or different FSAR design basis accident analysis. It does not introduce new equipment that could create a new or different kind of accident, and no new equipment failure modes are created. As a result, no new accident scenarios, failure mechanisms, or limiting single failures are introduced as a result of this proposed amendment.

   Therefore, the proposed amendment does not create a possibility for an accident of a new or different type than those previously evaluated.

3. Does the proposed amendment involve a significant reduction in a margin of safety?

   Response: No.

   The proposed amendment would not alter the way any safety-related SSC functions and would not alter the way the plant is operated. The amendment provides assurance that safety-related SSCs are protected from cyber attacks. The proposed amendment would not introduce any new uncertainties or change any existing uncertainties associated with any safety limit. The proposed amendment would have no impact on the structural integrity of the fuel cladding, reactor coolant pressure boundary, or containment structure. Based on the above considerations, the proposed amendment would not degrade the confidence in the ability of the fission product barriers to limit the level of radiation to the public.

   Therefore, the proposed change does not involve a significant reduction in a margin of safety.

Based on the above, NextEra concludes that the proposed amendment does not involve a significant hazards consideration under the standards set forth in 10 CFR 50.92(c), and, accordingly, a finding of "no significant hazards consideration" is justified.

4.3 Conclusions

In conclusion, based on the considerations discussed above: (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 amendment will not be inimical to the common defense and security or to the health and safety of the public.

5.0 ENVIRONMENTAL CONSIDERATION

The proposed amendment establishes the licensing basis for a Cyber Security Program for NextEra and will be a part of the Physical Security Plan. This proposed amendment will not involve any significant construction impacts. Pursuant to 10 CFR 51.22(c)(12) no environmental impact statement or environmental assessment need be prepared in connection with the issuance of the amendment.

6.0 REFERENCES

1. NextEra Energy Point Beach, LLC, letter to NRC, dated July 8, 2010, License Amendment Request 263A, Request for Approval of the Point Beach Plant Revised Cyber Security Plan (ML102720248)

2. Federal Register Notice, Final Rule 10 CFR Part 73, Power Reactor Security Requirements, published on March 27, 2009, 74 FR 13926.

3. EA-02-026, Order Modifying Licenses, Safeguards and Security Plan Requirements, issued February 25, 2002. (ML020510255)

ATTACHMENT 1 TO ENCLOSURE 2

NEXTERA ENERGY POINT BEACH, LLC
POINT BEACH NUCLEAR PLANT, UNITS 1 AND 2

SUPPLEMENT TO LICENSE AMENDMENT REQUEST 263,
RESPONSE TO REQUEST FOR ADDITIONAL INFORMATION

PROPOSED RENEWED FACILITY
OPERATING LICENSE CHANGES
UNITS 1 AND 2 (MARK-UP)

2 pages follow

D. Physical Protection

NextEra Energy Point Beach 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 combined set of plans, which contain Safeguards Information protected under 10 CFR 73.21, is entitled: "Point Beach Nuclear Plant Physical Security Plan, (Revision 4)," submitted by letter dated May 10, 2006. NextEra Energy Point Beach, LLC shall fully implement and maintain in effect all provisions of the Commission-approved Point Beach Nuclear Plant Cyber Security Plan submitted by letters dated July 8, 2010, supplemented by letter dated September 28, 2010, November 12, 2010, November 23, 2010, and March 31, 2011, and withheld from public disclosure in accordance with 10 CFR 2.390.

E. Safety Injection Logic

The licensee is authorized to modify the safety injection actuation logic and actuation power supplies and related changes as described in licensee's application for amendment dated April 27, 1979, as supplemented May 7, 1979. In the interim period until the power supply modification has been completed, should any DC powered safety injection actuation channel be in a failed condition for greater than one hour, the unit shall thereafter be shutdown using normal procedures and placed in a block-permissive condition for safety injection actuation.

F. NextEra Energy Point Beach shall implement and maintain in effect all provisions of the approved fire protection program as described in the FSAR for the facility and as approved in the Safety Evaluation Report dated August 2, 1979 (and Supplements dated October 21, 1980, January 22, 1981, and July 27, 1988) and the safety evaluation issued January 8, 1997, for Technical Specification Amendment No. 170, subject to the following provision:

> NextEra Energy Point Beach may make changes to the approved fire protection program without prior approval of the Commission only if those changes would not adversely affect the ability to achieve and maintain safe shutdown in the event of a fire.

G. Secondary Water Chemistry Monitoring Program

NextEra Energy Point Beach shall implement a secondary water chemistry monitoring program to inhibit steam generator tube degradation. This program shall include:

1. Identification of a sampling schedule for the critical parameters and control points for these parameters;
2. Identification of the procedures used to quantify parameters that are critical to control points;
3. Identification of process sampling points;
4. Procedure for the recording and management of data;
5. Procedures defining corrective actions for off control point chemistry condition; and

D. Physical Protection

NextEra Energy Point Beach 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 combined set of plans, which contain Safeguards Information protected under 10 CFR 73.21, is entitled: "Point Beach Nuclear Plant Physical Security Plan, (Revision 4)," submitted by letter dated May 10, 2006. NextEra Energy Point Beach, LLC shall fully implement and maintain in effect all provisions of the Commission-approved Point Beach Nuclear Plant Cyber Security Plan submitted by letters dated July 8, 2010, supplemented by letter dated September 28, 2010, November 12, 2010, November 23, 2010, and March 31, 2011, and withheld from public disclosure in accordance with 10 CFR 2.390.

E. Safety Injection Logic

The licensee is authorized to modify the safety injection actuation logic and actuation power supplies and related changes as described in licensee's application for amendment dated April 27, 1979, as supplemented May 7, 1979. In the interim period until the power supply modification has been completed, should any DC powered safety injection actuation channel be in a failed condition for greater than one hour, the unit shall thereafter be shut down using normal procedures and placed in a block-permissive condition for safety injection actuation.

F. NextEra Energy Point Beach shall implement and maintain in effect all provisions of the approved fire protection program as described in the FSAR for the facility and as approved in the Safety Evaluation Report dated August 2, 1979 (and Supplements dated October 21, 1980, January 22, 1981, and July 27, 1988) and the safety evaluation issued January 8, 1997, for Technical Specifications Amendment No. 174, subject to the following provision:

> NextEra Energy Point Beach may make changes to the approved fire protection program without prior approval of the Commission only if those changes would not adversely affect the ability to achieve and maintain safe shutdown in the event of a fire.

G. Secondary Water Chemistry Monitoring Program

NextEra Energy Point Beach shall implement a secondary water chemistry monitoring program to inhibit steam generator tube degradation. This program shall include:

1. Identification of a sampling schedule for the critical parameters and control points for these parameters;
2. Identification of the procedures used to quantify parameters that are critical to control points;
3. Identification of process sampling points;
4. Procedure for the recording and management of data;
5. Procedures defining corrective actions for off control point chemistry condition; and

ENCLOSURE 3

NEXTERA ENERGY POINT BEACH, LLC
POINT BEACH NUCLEAR PLANT, UNITS 1 AND 2

LICENSE AMENDMENT REQUEST 263
CYBER SECURITY PLAN

CYBER SECURITY PLAN IMPLEMENTATION MILESTONE SCHEDULE

Full implementation of the cyber security program involves many supporting tasks. Major activities include: program and procedure development; performing of individual critical digital asset (CDA) assessments; and identification, scheduling and implementing individual asset security control design remediation actions through the site configuration management program. These design modifications may be performed on-line or could require a refueling outage for installation.

The extensive workload associated with full implementation of the Cyber Security Plan (CSP) requires prioritization to assure those activities that provide higher degrees of protection against radiological sabotage are performed first. Therefore the CSP implementation schedule will be implemented with two major milestone dates. The first milestone date of no later than December 31, 2012, includes the activities listed in the table below. The second milestone date, December 31, 2015, includes the completion of all remaining actions that result in the full implementation of the cyber security plan for all applicable Safety, Security, and Emergency Preparedness (SSEP) functions. This date also bounds the completion of all individual asset security control design remediation actions.

Cyber security controls are not applied if the control adversely impacts safety and important to safety, security or emergency preparedness functions.

#	Implementation Milestone	Completion Date	Basis
1	Establish Cyber Security Assessment Team (CSAT) as described in Section 3.1.2 "Cyber Security Assessment Team" of the Cyber Security Plan (CSP).	No later than December 31, 2012	The CSAT, collectively, will need to have digital plant systems knowledge as well as nuclear power plant operations, engineering and nuclear safety experience and technical expertise. The personnel selected for this team may require additional training in these areas to ensure adequate capabilities to perform cyber security assessments as well as other duties.

#	Implementation Milestone	Completion Date	Basis
2	Identify Critical Systems (CSs) and Critical Digital Assets (CDAs) as described in Section 3.1.3 "Identification of Critical Digital Assets" of the CSP.	No later than December 31, 2012	The scope of 10 CFR 73.54 includes digital computer and communication systems and networks associated with: safety-related and important-to safety functions; security functions; emergency preparedness functions, including offsite communications; and support systems and equipment which, if compromised, would adversely impact safety, security, or emergency preparedness functions. The scope of 10 CFR 73.54 includes structures, systems, and components (SSCs) that have a nexus to radiological health and safety and therefore can directly or indirectly affect reactivity of a nuclear power plant and could result in an unplanned reactor shutdown or transient.
3	Implement installation of a deterministic one-way device between lower level devices (level 1, 2, and 3) and the higher level devices (level 4) as described in Section 4.3, "Defense-In-Depth Protective Strategies" of the CSP. Lower security level devices (level 1, 2, and 3 devices) that bypass the deterministic device and connect to level 4 will be modified to prevent the digital connectivity to the higher level or will be modified to meet cyber security requirements commensurate with the level 4 devices to which they connect. The design modifications that are not finished by the completion date will be documented in the site configuration management and/or change control program to assure completion of the design modification as soon as possible, but no later than the final implementation date.	No later than December 31, 2012	The implementation of communication barriers protects the most critical SSEP functions from remote attacks on plant systems. Isolating the plant systems from the internet as well as from the corporate business systems is an important milestone in defending against external threats. While the deployment of the barriers is critical to protection from external cyber threats, it also prevents remote access to core monitoring and plant data systems for reactor engineers, plant operations, and other plant staff. This elimination of remote access to reactor core monitoring systems may require the development and execution of a detailed change management plan to ensure continued safe operation of the plants. Vendors may be required to develop software revisions to support the model. The modification will be developed, prioritized and scheduled.

#	Implementation Milestone	Completion Date	Basis
4	The security control "Access Control For Portable And Mobile Devices" described in Appendix D 1.19 of NEI 08-09, Revision 6, will be implemented.	No later than December 31, 2012	Portable media devices are used to transfer electronic information (e.g., data, software, firmware, virus engine updates and configuration information) to and from plant process equipment. Careful use of this class of media is required to minimize the spread of malicious software to plant process equipment. The effective implementation of this control may require the coordinated implementation of other complimentary controls to ensure adequate mitigation.
5	Implement observation and identification of obvious cyber related tampering to existing insider mitigation rounds by incorporating the appropriate elements in Appendix E Section 4.3 "Personnel Performing Maintenance And Testing Activities."	No later than December 31, 2012	Insider mitigation rounds by trained staff look for obvious signs of cyber related tampering and would provide mitigation of observable cyber related insider actions. Implementing steps to add signs of cyber security-related tampering to insider mitigation rounds will be performed by the completion date.
6	Identify, document, and implement cyber security controls in accordance with the Cyber Security Plan Section 3.1.6 "Mitigation of Vulnerabilities and Application of Cyber Security Controls" for CDAs that could adversely impact the design function of physical security target set equipment. The implementation of controls that require a design modification that are not finished by the completion date will be documented in the site configuration management and/or change control program to assure completion of the design modification as soon as possible, but no later than the final implementation date.	No later than December 31, 2012	The site physical protection program provides high assurance that these elements are protected from physical harm by an adversary. The cyber security program will enhance the defense-in-depth nature of the protection of CDAs associated with target sets. Implementing Cyber Security Plan security controls for target set CDAs provides a high degree of protection against a cyber related attack that could lead to radiological sabotage. Security controls will be addressed in accordance with Cyber Security Plan Section 3.1.6, with the exception of those that require a design modification.

#	Implementation Milestone	Completion Date	Basis
7	Ongoing monitoring and assessment activities commence, as described in Section 4.4, "Ongoing Monitoring and Assessment" of the CSP, for those target set CDAs whose security controls have been implemented.	No later than December 31, 2012	The ongoing monitoring and assessment activities as described in Section 4.4, "Ongoing Monitoring and Assessment" of the Cyber Security Plan will be implemented for the controls applied to target set CDAs. This action results in the commencement of the cyber security program for target set related CDAs.
8	Full implementation of the NextEra Cyber Security Plan for all SSEP functions will be achieved.	No later than December 31, 2015	By the completion date, the Cyber Security Plan will be fully implemented for all SSEP functions in accordance with 10 CFR 73.54. This date also bounds the completion of all individual asset security control design remediation actions including those that require a refueling outage for implementation.