



November 23, 2010

NRC 2010-0183
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,
Request for Approval of the Point Beach Nuclear Plant
Revised Cyber Security Plan

- References:
- (1) NextEra Energy Point Beach, LLC, letter to NRC, dated July 8, 2009, License Amendment Request 263, Request for Approval of the Point Beach Plant Revised Cyber Security Plan (ML101900312)
 - (2) NextEra Energy Point Beach, LLC, letter to NRC, dated November 12, 2010, Supplement to License Amendment Request 263, Request for Approval of the Point Beach Nuclear Plant Revised Cyber Security Plan

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, 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 Cyber Security Plan.

In Reference (2), NextEra revised the Cyber Security Plan to clarify the scope of systems that will be protected under the provisions of the Plan.

The implementation schedule that was submitted with References (1) and (2) contained an error. Two milestones were inadvertently combined. Enclosure 1 contains the correct implementation schedule. This implementation schedule replaces the schedule provided in References (1) and (2).

The information contained in this letter does not alter the no significant hazards consideration contained in Reference (1) and (2) and continues to satisfy the criteria of 10 CFR 51.22 for categorical exclusion from the requirements of an environmental assessment.

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 November 23, 2010.

Very truly yours,

NextEra Energy Point Beach, LLC

A handwritten signature in black ink, appearing to read "Larry Meyer", with a long horizontal flourish extending to the right.

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 1

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

**LICENSE AMENDMENT REQUEST 263
CYBER SECURITY PLAN**

CYBER SECURITY PLAN PROPOSED IMPLEMENTATION SCHEDULE

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

**CYBER SECURITY PLAN
PROPOSED IMPLEMENTATION SCHEDULE**

Generic RAI Question 29 on NEI 08-09, Revision 3, Appendix A, includes reference to previous regulatory guidance and industry initiatives related to cyber security. As referenced, current industry guidance for cyber security is described in NEI 04-04, *Cyber Security Program for Power Reactors*. However, the scope of requirements in the NRC accepted implementation guidance contained in NEI 08-09, Revision 6, are significantly greater than the previously implemented cyber security program. The defensive model design requirements, the new digital asset assessment methodology, and the resultant digital asset remediation actions will require a significant expenditure of labor resources. As referenced in the Generic RAI Question 29, NextEra is also required to implement a separate cyber security program in accordance with the NERC Critical Infrastructure Protection Standards. While the timeframe for implementation is shorter for the NERC regulation, as described in the Generic RAI, the NERC cyber security methodology is different from the NRC Rule requirements. The NERC requirements are based on a logical risk based assessment process while the NRC Rule 73.54 requires a deterministic cyber security assessment methodology.

In light of the extensive work associated with implementation of these two new regulations, NextEra has developed a prioritized approach to establish the NRC Rule 73.54 implementation schedule. NextEra realizes the importance of deploying a uni-directional communication barrier to protect the most critical safety, security, and emergency preparedness (SSEP) functions. One major activity is the deployment of uni-directional communication barrier to ensure protection from remote attacks on plant systems. While the deployment of the uni-directional barrier is critical to protection from external cyber threats, it also impacts remote access to plant data systems by authorized personnel. This elimination of remote access will require Licensees to develop and implement a detailed change management plan.

Another major activity is the performance of individual critical digital asset (CDA) assessments to identify individual asset security control remediation actions. Programs and procedures are being developed to implement the programmatic requirements of the regulation. The cyber security assessment teams are also being established for execution of program requirements. These teams are required to have extensive knowledge of plant systems and cyber security control technology. A comprehensive training program will be required to ensure competent personnel for program execution.

The following implementation schedule includes implementation milestones and the date when NextEra proposes to complete the implementation and enter maintenance phase of the NRC approved Cyber Security Program.

Implementation Milestone	Completion Date	Basis
Cyber Security Assessment Team (CSAT) identified, trained and qualified. *	11/15/2010	<p>The CSAT will require a broad and very specialized knowledge of information and digital systems technology. The CSAT 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 will require additional training in these areas to ensure adequate capabilities to meet the regulation requirements.</p> <p>By the completion date, the following will be performed:</p> <ul style="list-style-type: none"> • Cyber security assessment procedures/tools will be developed and available; • Qualifications for CSAT will be developed; and • Training of the CSAT will be completed.
Develop Cyber Security Defensive Strategy (i.e., defensive model) *	02/04/2011	<p>The Defensive Strategy expands upon the high level model in the Cyber Security Plan and requires assessment of existing site and corporate policies, comparison to new requirements, revisions as required, and communication to plant personnel.</p> <p>By the completion date, the following will be performed:</p> <ul style="list-style-type: none"> • Documenting the defense-in-depth architecture and defensive strategy; • Revisions to existing defensive strategy policies will be implemented and communicated; and • Planning the implementation of the defense-in-depth architecture.
Critical System (CS) and Critical Digital Asset (CDA) identification complete*	06/15/2011	<p>By the completion date, the following will be performed:</p> <ul style="list-style-type: none"> • Critical Systems will be identified; and • Critical Digital Assets will be identified.
Deployment of uni-directional communication barrier to ensure protection from remote attacks on plant systems *	07/01/2012	<p>By the completion date, the following will be performed:</p> <ul style="list-style-type: none"> • The Defense in Depth Strategy will reflect implementation of the deterministic, one-way diode technology. • Engineering modifications required to configure, install and test the data diode will be completed.

Implementation Milestone	Completion Date	Basis
Final Cyber Security Assessments as described in the Cyber Security Plan completed and documented *	03/01/2013	<p>Based on the existing cyber security program, it is known that the number of digital assets requiring assessment is extensive. As previously discussed, the CDA assessment methodology required for this regulation is extremely rigorous and deterministic. The completion of these assessments will require a significant commitment of resources. The assessments will not begin prior to having a fully established CSAT and the required procedures.</p> <p>Performing the assessments will require participation of multiple disciplines and involve document reviews, system configuration evaluation, physical walk downs, or electronic verification of every communication pathway for each CDA, and documentation of results. These tasks will need to be coordinated and scheduled to align with department resource availability and system access requirements.</p> <p>By the completion date, the following will be performed:</p> <ul style="list-style-type: none"> • Cyber security assessments will be performed and documented.
Implementation of Cyber Security defense-in-depth architecture complete *	06/01/2013	<p>The implementation of communication barriers protects the most critical SSEP functions from remote attacks on our plant systems. 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 and other plant staff. This elimination of remote access to core monitoring systems requires the development and execution of a detailed change management plan to ensure continued safe operation of the plants.</p> <p>Vendors may be required to develop software revisions to support the defensive model. The modification will be developed, prioritized, and scheduled. Since software must be updated on and data retrieved from isolated systems, a method of patching, updating, and scanning isolated devices will be developed.</p>

Implementation Milestone	Completion Date	Basis
Establish Cyber Security Program policies/procedures *	07/01/2013	<p>The implementation of the cyber security program is expected to require policy/procedure development and/or upgrades for nearly every plant department. The procedural development for the cyber security program requirements and all of the individual security controls will be far-reaching. Many of the security controls will require development of the technical processes for implementing the control in a nuclear plant environment including development of new procedures for surveillances, periodic monitoring, and reviews. Procedure development will begin early in the implementation of the program and continue until the specified completion date.</p> <p>By the completion date, the following will be performed:</p> <ul style="list-style-type: none"> • Policies/procedures will be updated to establish Cyber Security Program; • The Cyber Security Assessment Procedure will be issued; and • New policies/procedures or revision of existing policies/procedures in areas impacted by cyber security requirements will be developed and implemented.
Implement all modifications (Outage and non Outage) and enter maintenance phase of NRC approved Cyber Security Program	12/31/2014	<p>The date when NextEra Point Beach proposes to complete the implementation and enter the maintenance phase of the NRC approved Cyber Security Program.</p> <ul style="list-style-type: none"> • All required modifications implemented • All required procedures updated • All required training completed

*Commitment changes will be managed in accordance with NEI 99-04, "Guidelines for Managing NRC Commitment Changes.