



November 7, 2014

NRC 2014-0067  
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 276  
Cyber Security Plan Milestone 8 Date Change Request

- References:
- (1) NextEra Energy Point Beach, LLC letter to NRC, License Amendment Request 263A, Request for Approval of the Point Beach Nuclear Plant Revised Cyber Security Plan, dated July 8, 2010, (ML101970011)
  - (2) NRC Letter to NextEra Energy Point Beach, LLC, Point Beach Nuclear Plant, Units 1 and 2 -Issuance of Amendments Re: Revised Cyber Security Plan (TAC NOS. ME4248 AND ME4249), dated July 21, 2011 (ML111740077)
  - (3) NextEra Energy Point Beach, LLC letter to NRC, License Amendment Request 276, Cyber Security Plan Milestone 8 Date Change Request, dated July 18, 2014 (ML14202A574)

In Reference (3), NextEra Energy Point Beach, LLC (NextEra) requested to amend the Cyber Security Plan for Point Beach Nuclear Plants, Units 1 and 2. The proposed change was a request to revise the completion date of Milestone 8 of the Cyber Security Plan implementation schedule. The Cyber Security Plan and implementation schedule were previously provided in Reference (1) and approved by the NRC in Reference (2).

Enclosure 1 provided a description and an evaluation of the proposed change. Enclosure 2 contained proposed marked-up operating license pages for the Physical Protection license condition for PBNP to reference the change requested in this submittal. Enclosure 3 contained the clean pages of the proposed revised operating license pages. Enclosure 1 contained security-related information (SRI), and NextEra requested Enclosure 1 be withheld from public disclosure in accordance with 10 CFR 2.390.

This supplement contains Enclosure 4 to License Amendment Request 276, which is a redacted version of Enclosure 1 that can be made available to the public.

There have been no changes to either the no significant hazards consideration or to the environmental considerations.

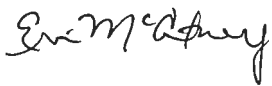
NextEra requests this license amendment be effective as of its date of issuance. Review and approval is requested by July 31, 2015.

A copy of this submittal is also being sent to our appointed state official pursuant to 10 CFR 50.91.

Should you have any questions regarding this submittal, please contact Mr. Michael Millen, Licensing Manager at 920/755-7845.

I declare under penalty of perjury that the foregoing is true and correct.  
Executed on November 7, 2014.

Very truly yours,



Eric McCartney  
Site Vice President

Enclosure

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

## **Enclosure 4**

### **Analysis of Proposed Operating License Change**

#### **Non-Security Related, Publically Available Version**

1. SUMMARY DESCRIPTION
2. DETAILED DESCRIPTION
3. BACKGROUND
4. TECHNICAL EVALUATION
5. REGULATORY EVALUATION
  - 5.1 Applicable Regulatory Requirements/Criteria
  - 5.2 No Significant Hazards Consideration Determination
  - 5.3 Conclusions
6. ENVIROMENTAL CONSIDERATION
7. REFERENCES

## 1. SUMMARY DESCRIPTION

NextEra Energy Point Beach, LLC (NextEra) requests an amendment to the Point Beach Nuclear Plants, (PBNP) Units 1 and 2 Renewed Facility Operating Licenses (FOL) Numbers DPR-24 and DPR-27 to change the scheduled completion date for Milestone 8 of the Cyber Security Plan (CSP) implementation schedule.

## 2. DETAILED DESCRIPTION

In References 1 and 2, the PBNP CSP and associated implementation schedule were approved by the NRC. Because the CSP implementation schedule contained in References 3 and 4 was utilized in the basis for the NRC safety evaluations (References 1 and 2), a License Amendment Request (LAR) is required to change the implementation schedule. This LAR includes a proposed change to the existing FOL for the PBNP Physical Protection License Condition. This Physical Protection License Condition change will reference the implementation schedule change for Milestone 8. [REDACTED]

[REDACTED] In accordance with the requirements identified in NRC memorandum dated October 24, 2013 (Reference 5), NextEra is requesting an extension of the PBNP CSP Milestone 8 completion date to [REDACTED].

## 3. BACKGROUND

Cyber security requirements are codified in 10 CFR 73.54 and are designed to provide high assurance that digital computer and communications 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). 10 CFR 73.54 specifically requires operating licenses implement a CSP that satisfies the requirements of the Rule in accordance with an NRC approved CSP implementation schedule.

On July 21, 2011, the NRC issued Amendments Numbers 243 and 247 for PBNP FOLs, respectively that approved the CSP and associated implementation schedule (Reference 1). On November 23, 2012, the NRC issued Amendments Numbers 247 and 251 for PBNP FOLs, respectively that approved a change to the in the Milestone 6 scope (Reference 2). NextEra underestimated the scope of the analysis involved with identification of critical digital assets (CDAs) and determination of the security controls to apply to these assets. The first seven milestones of the PBNP CSP implementation schedule have been completed. Implementation of the remainder of the CSP implementation schedule will require an extension of the Milestone 8 date.

## 4. TECHNICAL EVALUATION

This LAR proposes a change to the CSP Milestone 8 date of the PBNP CSP implementation schedule. In addition, the LAR includes proposed changes to the existing FOL condition for Physical Protection. The current license condition requires NextEra to fully implement the PBNP CSP by [REDACTED] in accordance with the CSP implementation schedule. The revised CSP implementation schedule proposes a completion date of [REDACTED].

The NRC provided criteria to be used for evaluation of a LAR revising the CSP Milestone 8 full implementation date in Reference 5. The following technical evaluation provides information concerning the eight criteria that serves to explain the current status of the PBNP CSP and the need to revise the Milestone 8 implementation date. The evaluation describes how prioritization

of NextEra's completed and planned implementation actions will provide 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) until the CSP is fully implemented by the proposed date.

**1. Identification of the specific requirements of the Cyber Security Program that Licensee needs additional time to implement.**

CSP Section 3.1, "Analyzing Digital Computer Systems and Networks Applying Cyber Security Controls"

[Redacted]

**2. Detailed justification that describes the reason Licensee requires additional time to implement the specific requirements identified.**

Detailed Justification for additional time to fully implement:

[Redacted]



[REDACTED]

[REDACTED]

[REDACTED]

**3. A proposed completion date for Milestone 8 consistent with the remaining scope of work to be conducted and the resources available.**

NextEra is requesting a change to the PBNP CSP Milestone 8 completion date from [REDACTED]. The date extension is requested in order to [REDACTED]. There is no change to the CSP other than this requested date change for Milestone 8.

The revised Milestone 8 date will encompass [REDACTED].

The revised completion date will help to avoid costly rework that could result from ongoing discussions between Nuclear Energy Institute (NEI) and NRC concerning the scope and application of CSP security controls.

**4. An evaluation of the impact of the additional time to implement the requirements will have on the effectiveness of Licensee's overall Cyber Security Program in the context of the milestones already completed.**

Based on the CSP program implementation activities already completed, and activities currently in progress, NextEra is secure and will continue to ensure that digital computer and communications systems and networks are adequately protected against cyber-attacks during implementation of the remainder of the program by the proposed Milestone 8 date of [REDACTED].

NextEra has completed implementation of Milestones 1 through 7 as required by [REDACTED]. Additionally, NextEra has completed the requirements of the "Good Faith Letter" (Reference 6). Any identified discrepancies are being addressed through the corrective action program (CAP). A discussion of cyber security related issues in CAP is contained in paragraph 7 below. The completed activities provide a high degree of protection against cyber-attacks while NextEra implements the full CSP. The completed activities include:

[REDACTED]

[REDACTED]

[REDACTED]





[REDACTED]

The additional time requested to complete Milestone 8 will not impact the overall effectiveness of the CSP. Considering the CSP currently in place, the completed Milestone 1 through 7, implementation of the "Good Faith Letter" actions, and completion of prioritized activities in progress, there is minimal impact to PBNP's safe and reliable power operation. The extended Milestone 8 date will allow for completion of the remaining activities and modifications. The revised date encompasses [REDACTED] for implementation of modifications required as a result of CDA assessments. The Milestone 8 extension will provide time to fully integrate the CSP into plant programs, processes, procedures, and training.

**5. A description of Licensee’s methodology for prioritizing completion of work for critical digital assets (CDAs) associated with significant safety, security, or emergency preparedness (EP) consequences and with reactivity effects in the balance of plant (BOP).**

NextEra’s methodology for prioritizing Milestone 8 activities is centered on considerations for safety, security, EP, and BOP (continuity of power) consequences. The methodology is based on [REDACTED]

[REDACTED]

**6. A discussion of Licensee’s Cyber Security Program performance up to the date of the LAR.**

Milestones 1 through 7 activities were completed by [REDACTED], and all actions from the NRC “Good Faith” letter have been implemented. Any identified discrepancies are being addressed through the CAP. A discussion of cyber security related issues in CAP is contained in paragraph 7 below. These activities provide a high degree of protection against cyber security related attacks until such time that the full program is implemented. These activities include:

Portable Device/Mobile Computing Device Control Program:

- Overall implementation is effective. PBNP has documented in the CAP corrective actions [REDACTED].

Defense-In-Depth and Diodes (Level 4 – Level 3):

[REDACTED]

- Overall integrity of implemented modifications is effective based on CAP data.

NextEra has completed a comprehensive self-assessment for milestones 1 through 7 implementation, including the NRC Good Faith action items, to ensure completeness and effectiveness. Self-assessment issues were entered into the CAP and addressed for program improvement.

Ongoing monitoring and periodic actions provide continuing program performance monitoring.

**7. A discussion of cyber security issues pending in NextEra's Corrective Action Program.**

The PBNP CAP is used to document all cyber issues in order to trend, correct, and improve NextEra's CSP. The CAP database documents and tracks, from initiation to closure, all cyber security required actions, including issues identified during ongoing program assessment activities. Adverse trends are monitored for program improvement and addressed via the CAP process. Examples of issues and activities pending in the CAP which are related to cyber security include:

AR Number	OPEN Corrective Actions
[REDACTED] 01928177 [REDACTED]	[REDACTED]

**8. A discussion of modifications completed to support the Cyber Security Program and a discussion of pending Cyber Security modifications.**

The following modifications have been completed in support of the CSP:  
[REDACTED]

Mitigations identified to date will be made to the following systems and equipment in support of the CSP:  
[REDACTED]  
[REDACTED]



**5. REGULATORY EVALUATION**

**5.1 Applicable Regulatory Requirements/Criteria**

10 CFR 73.54 requires licensees to maintain and implement a Cyber Security Plan (CSP). Point Beach Nuclear Plant, Units 1 and 2 (PBNP) Renewed Facility Operating Licenses (FOL) Nos. DPR-24 and DPR-27 include a Physical Protection License Condition that requires NextEra Energy Point Beach, LLC (NextEra) to fully implement and maintain in effect all provisions of the Commission-approved CSP, including changes made pursuant to the authority of 10 CFR 50.90 and 10 CFR 50.54(p).

**5.2 No Significant Hazards Consideration Determination**

NextEra is requesting approval of changes to PBNP FOLs DPR-24 and DPR-27 to revise the Physical Protection License Condition as it relates to the Cyber Security Plan. This change includes a proposed deviation to the Cyber Security Plan implementation schedule and a proposed revision to the PBNP FOL Nos. DPR-24 and DPR-27, respectively to revise the Physical Protection License Condition as it relates to the Cyber Security Plan. This change includes a proposed deviation to the Cyber Security Plan implementation schedule and a proposed revision to the PBNP FOLs to include the proposed deviation. Specifically, NextEra proposes to change the completion date for full implementation (Milestone 8) of the Cyber Security Plan.

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 described below:

- (1) Does the proposed change involve a significant increase in the probability or consequences of an accident previously evaluated?

Response: No.

The proposed change to the Cyber Security Plan implementation schedule does not alter accident analysis assumptions, add any initiators, or affect the function of plant systems or the manner in which systems are operated, maintained, tested, or inspected. The proposed change does not require any plant modifications which affect the performance capability or the structures, systems, and components relied upon to mitigate the consequences of postulated accidents and has no impact on the probability or consequences of an accident previously evaluated.

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

- (2) Does the proposed change create the possibility of a new or different kind of accident from any accident previously evaluated?

Response: No.

The proposed change to the Cyber Security Plan implementation schedule does not alter accident analysis assumptions, add any initiators, or affect the function of plant systems or the manner in which systems are operated, maintained, modified, tested, or inspected. The proposed change does not require any plant modifications which affect the performance capability of the structures, systems, and components relied upon to mitigate the consequences of postulated accidents and does not create the possibility of a new or different kind of accident from any accident previously evaluated.

Therefore, the proposed change does not create the possibility of a new or different kind of accident from any accident previously evaluated.

- (3) Does the proposed change involve a significant reduction in a margin of safety?

Response: No.

Plant safety margins are established through limiting conditions of operation, limiting safety systems settings, and safety limits specified in the Technical Specifications. The proposed change to the Cyber Security Plan implementation schedule does not change these established safety margins as result of this change, the proposed change does not involve a significant reduction in a margin of safety.

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

Based on the above, NextEra concludes that the proposed change presents no 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.

### 5.3 Conclusion

Based on the considerations described 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 in compliance with the Commission's regulations, and (3) the issuance of amendments will not be inimical to the common defense and security or to the health and safety of the public.

## **6. ENVIRONMENTAL CONSIDERATION**

The proposed amendment provides a change to the Cyber Security Plan implementation schedule. The proposed amendment meets the eligibility criterion for a categorical exclusion set forth in 10 CFR 51.22(c)(12). Therefore, pursuant to 10 CFR 51.22(b), no environmental impact statement or environmental assessment need be prepared in connection with the issuance of this amendment.

## **7. REFERENCES**

1. NRC Letter to NextEra Energy Point Beach, LLC, Point Beach Nuclear Plant, Units 1 and 2 -Issuance of Amendments Re: Revised Cyber Security Plan (TAC NOS. ME4248 AND ME4249), dated July 21, 2011 (ML111740077)
2. NRC letter to NextEra Energy Point Beach, LLC, Point Beach Nuclear Plant, Units 1 and 2 -Issuance of Amendments Re: Revised Cyber Security Plan Implementation Schedule Milestone 6 (TAC NOS. ME8914 and ME8915), dated November 23, 2012, (ML12251A155)
3. NextEra Energy Point Beach, LLC letter to NRC, License Amendment Request 263A, Request for Approval of the Point Beach Nuclear Plant Revised Cyber Security Plan, dated July 8, 2010, (ML101970011)
4. NextEra Energy Point Beach, LLC letter to NRC, License Amendment Request 269 Cyber Security Plan Implementation Schedule Milestone Change, dated June 18, 2012, (ML12172A386)
5. NRC memorandum to R. Felts (NRC), Review Criteria for Title 10 of the Code of Federal Regulations Part 73.54, Cyber Security Implementation Schedule Milestone 8 License Amendment Requests, dated October 24, 2013 (ML13295A467)
6. NRC memorandum to C. Miller et al. (NRC), Enhanced Guidance for Licensee Near-Term Corrective Actions to Address Cyber Security Inspection Findings and Licensee Eligibility for "Good Faith" Attempt Discretion, dated July 1, 2013, (ML13178A203)