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

June 6, 2016

Vice President, Operations
Entergy Nuclear Operations, Inc.
Pilgrim Nuclear Power Station
600 Rocky Hill Road
Plymouth, MA 02360-5508

SUBJECT: PILGRIM NUCLEAR POWER STATION - ISSUANCE OF AMENDMENT RE: CYBER SECURITY PLAN IMPLEMENTATION SCHEDULE (CAC NO. MF6517)

Dear Sir or Madam:

The U.S. Nuclear Regulatory Commission (the Commission) has issued the enclosed Amendment No. 244 to Renewed Facility Operating License No. DPR-35 for the Pilgrim Nuclear Power Station. The amendment consists of changes to the Cyber Security Plan (CSP) Milestone 8 full implementation date in response to your application dated July 15, 2015.

The amendment revises the CSP Milestone 8 full implementation date by extending the date from June 30, 2016, to December 15, 2017. The amendment also revises paragraphs 3.B and 3.G of the renewed facility operating license to incorporate the revised CSP implementation schedule.

A copy of the related Safety Evaluation is enclosed. A Notice of Issuance will be included in the Commission's biweekly *Federal Register* Notice.

Sincerely,

Brenda Mozafari for

Booma Venkataraman, Project Manager
Plant Licensing Branch I-1
Division of Operating Reactor Licensing
Office of Nuclear Reactor Regulation

Docket No. 50-293

Enclosures:
1. Amendment No. 244 to Renewed License No. DPR-35
2. Safety Evaluation

cc w/encls: Distribution via Listserv

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

ENTERGY NUCLEAR GENERATION COMPANY

AND ENTERGY NUCLEAR OPERATIONS, INC.

PILGRIM NUCLEAR POWER STATION

DOCKET NO. 50-293

AMENDMENT TO RENEWED FACILITY OPERATING LICENSE

Amendment No. 244
Renewed License No.
DPR-35

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

   A. The application for amendment filed by Entergy Nuclear Operations, Inc. (the licensee) dated July 15, 2015, complies with the standards and requirements of the Atomic Energy Act of 1954, as amended (the Act), and the Commission's rules and regulations;

   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.

2. Accordingly, the license is amended by changes to paragraph 3.B and 3.G of Renewed Facility Operating License No. DPR-35.

Paragraph 3.B is hereby amended to read as follows:

B. Technical Specifications

The Technical Specifications contained in Appendix A, as revised through Amendment No. 244, are hereby incorporated in the renewed operating license. The licensee shall operate the facility in accordance with the Technical Specifications.

The second paragraph of Paragraph 3.G is hereby amended to read as follows:

G. Physical Protection

The licensee 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 licensee's CSP was approved by License Amendment No. 236, as supplemented by changes approved by License Amendment Nos. 238, 241 and 244.

4. This license amendment is effective as of the date of issuance and shall be implemented within 30 days from the date of issuance. The full implementation of the CSP shall be in accordance with the implementation schedule submitted by the licensee on July 15, 2015, and approved by the NRC staff with this license amendment. All subsequent changes to the NRC-approved CSP implementation schedule will require NRC approval pursuant to 10 CFR 50.90.

FOR THE NUCLEAR REGULATORY COMMISSION

Travis L. Tate, Chief
Plant Licensing Branch I-1
Division of Operating Reactor Licensing
Office of Nuclear Reactor Regulation

Attachment:
Changes to the Renewed Facility
Operating License No. DPR-35

Date of Issuance: June 6, 2016

ATTACHMENT TO LICENSE AMENDMENT NO. 244

RENEWED FACILITY OPERATING LICENSE NO. DPR-35

DOCKET NO. 50-293

Replace the following page of the Renewed Facility Operating License with the attached revised page. The revised page is identified by amendment number and contains marginal lines indicating the areas of change.

Remove	Insert
Page 3	Page 3

provisions of the Act and to the rules, regulations, and orders of the Commission now or hereafter in effect; and is subject to the additional conditions specified below:

A. Maximum Power Level

ENO is authorized to operate the facility at steady state power levels not to exceed 2028 megawatts thermal.

B. Technical Specifications

The Technical Specifications contained in Appendix A, as revised through Amendment No. 244 are hereby incorporated in the renewed operating license. The licensee shall operate the facility in accordance with the Technical Specifications.

C. Records

ENO shall keep facility operating records in accordance with the requirements of the Technical Specifications.

D. Equalizer Valve Restriction - DELETED

E. Recirculation Loop Inoperable – DELETED

F. Fire Protection

ENO shall implement and maintain in effect all provisions of the approved fire protection program as described in the Final Safety Analysis Report for the facility and as approved in the SER dated December 21, 1978 as supplemented subject to the following provision:

ENO 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. Physical Protection

The licensee shall fully implement and maintain in effect all provisions of the Commission-approved physical security, training and qualification, and safeguards contingency plans including amendments made pursuant to provisions of the Miscellaneous Amendments and Search Requirements revisions to 10 CFR 73.55 (50 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: "Pilgrim Nuclear Power Station Physical Security, Training and Qualification, and Safeguards Contingency Plan, Revision 0" submitted by letter dated October 13, 2004, as supplemented by letter dated May 15, 2006.

The licensee 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 licensee's CSP was approved by License Amendment No. 236, as supplemented by changes approved by: License Amendment Nos. 238, 241, and 244.

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

SAFETY EVALUATION BY THE OFFICE OF NUCLEAR REACTOR REGULATION

RELATED TO AMENDMENT NO. 244

TO RENEWED FACILITY OPERATING LICENSE NO. DPR-35

ENTERGY NUCLEAR GENERATION COMPANY

AND ENTERGY NUCLEAR OPERATIONS, INC.

PILGRIM NUCLEAR POWER STATION

DOCKET NO. 50-293

1.0 INTRODUCTION

By application dated July 15, 2015 (Agencywide Documents Access and Management System (ADAMS) Accession No. ML15205A287), Entergy Nuclear Operations, Inc. (ENO, the licensee) requested a change to the renewed facility operating license for Pilgrim Nuclear Power Station (PNPS). The proposed change would revise the completion date of the PNPS Cyber Security Plan (CSP) by extending the date for full implementation from June 30, 2016, to December 15, 2017. The proposed change would also revise Paragraph 3.G in the renewed facility operating license.

The U.S. Nuclear Regulatory Commission (NRC) staff reviewed and approved the licensee's original CSP implementation schedule for PNPS by letter dated July 22, 2011, Amendment No. 236 (ADAMS Accession No. ML11152A043), concurrent with the incorporation of the CSP into the facility's current licensing basis. Subsequently, by application dated January 31, 2014 (ADAMS Accession No. ML14042A166), as supplemented by letter dated July 1, 2014 (ADAMS Accession No. ML14195A008), the licensee requested an extension to the date of the CSP implementation schedule. By letter dated December 11, 2014 (ADAMS Accession No. ML14336A661), the NRC staff approved the extension to the implementation schedule in Amendment No. 241. This schedule required the licensee to fully implement and maintain all provisions of the CSP for PNPS no later than June 30, 2016.

The NRC issued a proposed finding that the amendment involves no significant hazards consideration in the *Federal Register* on October 27, 2015 (80 FR 65812). The NRC did not receive public comments on this determination.

2.0 REGULATORY EVALUATION

The NRC staff considered the following regulatory requirements and guidance in its review of the license amendment request (LAR) to modify the existing CSP implementation schedule:

- Title 10 of the *Code of Federal Regulations* (10 CFR), Section 73.54, "Protection of digital computer and communication systems and networks," which states, in part:

  > Each [CSP] submittal must include a proposed implementation schedule. Implementation of the licensee's cyber security program must be consistent with the approved schedule.

- The licensee's renewed facility operating license includes a license condition that requires the licensee to fully implement and maintain in effect all provisions of the Commission-approved CSP.

- NRC memorandum, "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 (ADAMS Accession No. ML13295A467), in which the NRC staff lists criteria to consider during evaluations of licensees' requests to postpone their cyber security program implementation date (commonly known as Milestone 8).

The NRC staff does not regard the CSP milestone implementation dates as regulatory commitments that can be changed unilaterally by the licensee, particularly in light of the regulatory requirement at 10 CFR 73.54, that states, "Implementation of the licensee's cyber security program must be consistent with the approved schedule." As the NRC staff explained in its letter to all operating reactor licensees dated May 9, 2011 (ADAMS Accession No. ML110980538), the implementation of the plan, including the key intermediate milestone dates and the full implementation date shall be in accordance with the implementation schedule submitted by the licensee and approved by the NRC. All subsequent changes to the NRC-approved CSP implementation schedule, thus, will require prior NRC approval as required by 10 CFR 50.90, "Application for amendment of license, construction permit, or early site permit."

3.0 TECHNICAL EVALUATION

3.1 Licensee's Requested Change

The NRC staff issued Amendment No. 236 to Renewed Facility Operating License DPR-35 for PNPS by letter dated July 22, 2011. This amendment approved the licensee's CSP and associated implementation schedule, and added a sentence to the license condition requiring the licensee to fully implement and maintain the Commission-approved CSP. The licensee's implementation schedule was based on a template prepared by the Nuclear Energy Institute (NEI), which was transmitted to the NRC by letter dated February 28, 2011 (ADAMS Accession No. ML110600206). By letter dated March 1, 2011, the NRC staff found the NEI template acceptable for licensees to use to develop their CSP implementation schedules (ADAMS Accession No. ML110070348). The licensee's proposed implementation schedule for the CSP identified completion dates and bases for the following eight milestones:

1) Establish the Cyber Security Assessment Team (CSAT);

2) Identify Critical Systems (CSs) and Critical Digital Assets (CDAs);

3) Install deterministic one-way devices between lower level devices and higher level devices;

4) Implement the security control "Access Control For Portable And Mobile Devices";

5) Implement observation and identification of obvious cyber related tampering to existing insider mitigation rounds by incorporating the appropriate elements;

6) Identify, document, and implement technical cyber security controls in accordance with "Mitigation of Vulnerabilities and Application of Cyber Security Controls" for CDAs that could adversely impact the design function of physical security target set equipment;

7) Ongoing monitoring and assessment activities for those target set CDAs whose security controls have been implemented;

8) Fully implement the CSP.

Currently, Milestone 8 of the PNPS CSP requires the licensee to fully implement the CSP by June 30, 2016. By application dated July 15, 2015, the licensee proposed to modify the Milestone 8 completion date to December 15, 2017.

The licensee submitted its application, using the NRC staff's guidance to evaluate requests to postpone Milestone 8 implementation dates. The licensee's application addressed all the criteria in the guidance. The intent of the staggered cyber security implementation schedule was for licensees to demonstrate ongoing implementation of their cyber security program prior to full implementation, which was scheduled for the date specified in Milestone 8. The licensee completed seven other milestones (Milestone 1 through Milestone 7) by December 31, 2012. Activities included establishing a CSAT, identifying CSs and CDAs, installing deterministic one-way devices between defensive levels, implementing access control for portable and mobile devices, implementing methods to observe and identify obvious cyber-related tampering, and conducting ongoing monitoring and assessment activities for target set CDAs. In their aggregate, the interim milestones demonstrate ongoing implementation of the cyber security program.

The licensee provided the following information pertinent to each of the criteria identified in the NRC guidance memorandum dated October 24, 2013:

1) Identification of the specific requirement or requirements of the cyber security plan that the licensee needs additional time to implement.

   The licensee stated that the following requirements of the CSP require additional time for implementation: Section 3, "Analyzing Digital Computer Systems and Networks," and Section 4, "Establishing, Implementing and Maintaining the Cyber Security Program." The licensee further noted that these sections describe the process for application and maintenance of cyber security controls and the process of addressing security controls.

2) Detailed justification that describes the reason the licensee requires additional time to implement the specific requirement or requirements identified.

The licensee stated it had hosted a "pilot" Milestone 8 inspection at the Indian Point Energy Center in March 2014. During the pilot, insight was gained into the NRC perspective on how to apply the cyber security controls listed in NEI 08-09, "Cyber Security Plan for Nuclear Power Reactors", Revision 6, dated April 2010 (ADAMS Accession No. ML101180437). During the pilot inspection, the NRC team reviewed several examples of CDAs with ENO and indicated the level of detail and depth expected in the technical analyses for cyber security controls referenced in NEI 08-09. Based on this review, ENO stated that the detail and depth of the technical analysis exceeds ENO's prior understanding and necessitates a greater effort to achieve than initially anticipated.

The licensee stated that during 2015, each operating ENO licensee had an inspection of compliance with interim Milestones 1 through 7. The preparation for and support of these inspections required a significant commitment of time from ENO's most knowledgeable subject matter experts on nuclear cyber security, exceeding the estimate previously developed and thereby, drawing those resources away from Milestone 8 implementation activities.

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

   The licensee proposed a Milestone 8 completion date of December 15, 2017.

4) An evaluation of the impact that the additional time to implement the requirements will have on the effectiveness of the licensee's overall cyber security program in the context of milestones already completed.

   The licensee indicated that the impact of the requested additional implementation time on the effectiveness of the overall cyber security program is very low, because the milestones already completed have resulted in a high degree of protection of safety-related, important-to-safety, and security CDAs against common threat vectors. Additionally, the licensee stated that extensive physical and administrative measures are already in place for CDAs because they are plant components, pursuant to the PNPS Security Plan and Technical Specification requirements.

   The licensee then provided details about implementation of Milestones 1 through 8.

5) A description of the licensee's methodology for prioritizing completion of work for critical digital assets associated with significant safety, security or emergency preparedness (SSEP) consequences and with reactivity effects in the balance of plant.

   The licensee stated because CDAs are plant components, prioritization follows the normal work management process that places the highest priority on apparent conditions adverse to quality in system, structure, and component design function and related factors such as safety risk and nuclear defense-in-depth, as well as threats to continuity of electric power generation in the balance-of-plant (BOP). High focus continues to be maintained on prompt attention to any emergent issue with these CDAs that would potentially challenge the established cyber protective barriers. Additionally,

it should be noted that these CDAs encompass those associated with physical security target sets.

6) A discussion of the licensee's cyber security program performance up to the date of the license amendment request.

   The licensee stated there has been no identified compromise of SSEP functions by cyber means. It also noted a formal Quality Assurance (QA) audit was conducted in the last quarter of 2014. The QA audit included a review of the cyber security program implementation. There were no significant findings related to cyber security program performance and effectiveness.

7) A discussion of cyber security issues pending in the licensee's corrective action program (CAP).

   The licensee stated there are presently no significant (constituting a threat to a CDA via cyber means or calling into question program effectiveness) nuclear cyber security issues pending in the PNPS CAP. However, several non-significant issues identified during the QA audit described above and identified during NRC inspections have been entered into CAP.

8) A discussion of modifications completed to support the cyber security program and a discussion of pending cyber security modifications.

   The licensee provided a brief discussion of a completed modification and pending modifications.

3.2 NRC Staff Evaluation

The NRC staff has evaluated the licensee's application using the regulatory requirements and guidance above. The NRC staff's evaluation is below. The NRC staff finds that the actions the licensee noted as being required to implement the CSP, Section 3, "Analyzing Digital Computer Systems and Networks," and Section 4, "Establishing, Implementing and Maintaining the Cyber Security Program" are reasonable as discussed below.

The licensee indicated that completion of the activities associated with the CSP, as described in Milestones 1 through 7 were completed prior to December 31, 2012, and provide a high degree of protection to ensure that the most significant digital computer and communication systems and networks associated with SSEP functions are protected against cyber attacks. The NRC staff finds that the licensee's site is more secure after the implementation of Milestones 1 through 7 because the activities the licensee has completed mitigate the most significant cyber attack vectors for the most significant CDAs.

The licensee stated that the detail and depth of the technical analysis exceeds ENO's prior understanding and necessitates a greater effort to achieve than Entergy anticipated when the current implementation schedule was developed. The NRC staff recognizes that CDA assessment work, including application of controls is more complex and resource intensive than Entergy anticipated. As a result, the licensee has a large number of additional tasks not considered when developing its current CSP implementation schedule. The staff concludes that

the licensee's request for additional time to implement Milestone 8 is reasonable, given the complexity, volume, and scope of the remaining work required to fully implement its CSP.

The licensee proposed a Milestone 8 completion date of December 15, 2017. The licensee's prioritization of completion of work for CDAs follows the normal work management process that places the highest priority on apparent conditions adverse to quality in system, structure, and component design function and relates to factors such as safety risk and nuclear defense-in-depth. High focus continues to be maintained on prompt attention to any emergent issue with safety-related, security, and important to safety (including BOP) CDAs that would potentially challenge the established cyber protective barriers. The NRC staff concludes that the licensee's methodology for prioritizing work on CDAs is appropriate. The NRC staff further finds that the licensee's request to delay final implementation of the CSP until December 15, 2017, is reasonable given the complexity of the remaining work and the licensee's resource constraints.

3.2 Technical Evaluation Conclusion

Based on its review of the licensee's submittal, the NRC staff concludes that the licensee's request to delay full implementation of its CSP until December 15, 2017, is reasonable for the following reasons: (i) the licensee's implementation of Milestones 1 through 7 provides mitigation for significant cyber attack vectors for the most significant CDAs as discussed in the staff evaluation above; (ii) the scope of the work required to come into full compliance with the CSP implementation schedule was more complicated than the licensee anticipated when the current CSP implementation schedule was developed; and (iii) the licensee has reasonably prioritized and scheduled the work required to come into full compliance with its CSP implementation schedule. Therefore, the staff finds the proposed change acceptable.

3.3 Revision to License Condition 3.G

The licensee proposed to modify Paragraph 3.G of Renewed Facility Operating License No. DPR-35 for PNPS, which provides a license condition to require the licensee to fully implement and maintain in effect all provisions of the Commission-approved CSP.

The current license condition in Paragraph 3.G of Renewed Facility Operating License No. DPR-35 for PNPS states, in part:

> The licensee 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 licensee's CSP was approved by License Amendment No. 236, as supplemented by changes approved by License Amendment Nos. 238 and 241.

The revised license condition in Paragraph 3.G of Renewed Facility Operating License No. DPR-35 for PNPS would state:

> The licensee 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 licensee's

CSP was approved by License Amendment No. 236, as supplemented by changes approved by License Amendment Nos. 238, 241 and 244.

Based on the information in Section 3.0 of this safety evaluation and the modified license condition described above, the NRC staff concludes that the proposed schedule change is acceptable.

4.0 REGULATORY COMMITMENTS

By letter dated July 15, 2015, the licensee made the following regulatory commitment:

> Full implementation of Pilgrim Nuclear Power Station Cyber Security Plan for all safety, security, and emergency preparedness functions will be achieved.
>
> Scheduled Completion Date: December 15, 2017

The above stated commitment is consistent with the revised Milestone 8 implementation date proposed by the licensee and evaluated by the NRC staff.

4.0 STATE CONSULTATION

In accordance with the Commission's regulations, the Massachusetts State official was notified of the proposed issuance of the amendment. The State official had questions on the proposed amendment and NRC addressed the questions by email dated April 13, 2016 (ADAMS Accession No. ML16105A049).

5.0 ENVIRONMENTAL CONSIDERATION

This is an amendment to a 10 CFR Part 50 license that relates solely to safeguards matters and does not involve any significant construction impacts. This amendment is an administrative change to extend the date by which the licensee must have its CSP fully implemented. Accordingly, the amendment meets the eligibility criteria for categorical exclusion set forth in 10 CFR 51.22(c)(12). Pursuant to 10 CFR 51.22(b), no environmental impact statement or environmental assessment need be prepared in connection with the issuance of the amendment.

6.0 CONCLUSION

The Commission has concluded, based on the considerations discussed above, that: (1) there is reasonable assurance that the health and safety of the public will not be endangered by operation in the proposed manner, (2) 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.

Principal Contributor: John Rycyna, NSIR

Date: June 6, 2016.

June 6, 2016

Vice President, Operations
Entergy Nuclear Operations, Inc.
Pilgrim Nuclear Power Station
600 Rocky Hill Road
Plymouth, MA 02360-5508

SUBJECT: PILGRIM NUCLEAR POWER STATION - ISSUANCE OF AMENDMENT RE: CYBER SECURITY PLAN IMPLEMENTATION SCHEDULE (CAC NO. MF6517)

Dear Sir or Madam:

The U.S. Nuclear Regulatory Commission (the Commission) has issued the enclosed Amendment No. 244 to Renewed Facility Operating License No. DPR-35 for the Pilgrim Nuclear Power Station. The amendment consists of changes to the Cyber Security Plan (CSP) Milestone 8 full implementation date in response to your application dated July 15, 2015.

The amendment revises the CSP Milestone 8 full implementation date by extending the date from June 30, 2016, to December 15, 2017. The amendment also revises paragraphs 3.B and 3.G of the renewed facility operating license to incorporate the revised CSP implementation schedule.

A copy of the related Safety Evaluation is enclosed. A Notice of Issuance will be included in the Commission's biweekly *Federal Register* Notice.

Sincerely,
/RA BMozafari for/
Booma Venkataraman, Project Manager
Plant Licensing Branch I-1
Division of Operating Reactor Licensing
Office of Nuclear Reactor Regulation

Docket No. 50-293

Enclosures:
1. Amendment No. 244 to Renewed License No. DPR-35
2. Safety Evaluation

cc w/encls: Distribution via Listserv

DISTRIBUTION:
PUBLIC
LPL1-1 R/F
RidsNrrDorlDpr Resource
RidsRgn1MailCenter Resource
RidsNrrDorlLpll-1 Resource
RidsNsir Resource
JBeardsley, NSIR
RidsACRS_MailCTR Resource
RidsNrrLAKGoldstein Resource
RidsNrrDssStsbResource
RidsNrrPMPilgrim Resource
RecordsAmend
JRycyna, NSIR

ADAMS Accession No.: ML16082A460

OFFICE	NRR/DORL/LPL1-1/PM	NRR/DORL/LPL1-1/LA	NSIR/CSD/D
NAME	BVenkataraman	KGoldstein	JBeardsley (by email)
DATE	05/27/16	05/02/16	02/23/2016
OFFICE	OGC- NLO	NRR/DORL/LPLI-1/BC	NRR/DORL/LPL1-1/PM
NAME	JBielecki	TTate	BVenkarataman (BMozafari for)
DATE	04/26/2016	06/06/2016	06/06/2016

OFFICIAL RECORD COPY