



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

John A. Dent, Jr.
Site Vice President

July 15, 2015

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

SUBJECT: License Amendment Request – Cyber Security Plan Implementation Schedule
Pilgrim Nuclear Power Station (PNPS)
Docket Nos. 50-293
License Nos. DPR-35

- REFERENCES:
1. NRC Internal Memorandum to Barry Westreich from Russell Felts, "Review Criteria for 10 CFR 73.54, Cyber Security Implementation Schedule Milestone 8 License Amendment Requests," dated October 24, 2013 (ML13295A467)
 2. NRC letter to Entergy, "Issuance of Amendment To Facility Operating License Re: Cyber Security Plan," dated July 22, 2011 (PNPS Letter 1.11.048) (ML11152A043)
 3. NRC letter to Entergy, "Issuance of Amendment Regarding Cyber Security Plan Implementation Schedule Milestone 8," dated December 11, 2014 (PNPS Letter 1.14.083) (ML14336A661)

PNPS Letter 2.15.045

Dear Sir or Madam:

Pursuant to 10 CFR 50.4 and 10 CFR 50.90, Entergy Nuclear Operations, Inc. (Entergy) hereby requests an amendment to the Renewed Facility Operating Licenses for Pilgrim Nuclear Power Station (PNPS). In accordance with the guidelines provided by Reference 1, this request proposes a change to the PNPS Cyber Security Plan Milestone 8 full implementation date as set forth in the Cyber Security Plan Implementation Schedule approved by References 2 and 3.

Attachment 1 provides an evaluation of the proposed change. Attachment 2 contains proposed marked-up operating license pages for the Physical Protection license condition for PNPS to reference the commitment change provided in this submittal.

S001A
NRR

Attachment 3 contains the proposed revised operating license pages. Attachment 4 contains a change to the date of Implementation Milestone 8.

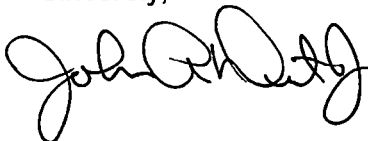
The proposed changes have been evaluated in accordance with 10 CFR 50.91(a)(1) using criteria in 10 CFR 50.92(c), and it has been determined that the changes involve no significant hazards consideration. The bases for these determinations are included in Attachment 1.

Entergy requests this license amendment be effective as of its date of issuance. Although this request is neither exigent nor emergency, your review and approval is requested prior to June 30, 2016.

The revised commitment contained in this submittal is summarized in Attachment 5. Should you have any questions concerning this letter, or require additional information, please contact Mr. Everett (Chip) Perkins at (508) 830-8323.

I declare under penalty of perjury that the foregoing is true and correct. Executed on July 15, 2015.

Sincerely,

A handwritten signature in black ink, appearing to read "John A. Dent Jr.", with a stylized, cursive script.

John A. Dent Jr.
Site Vice President

JAD/rmb

- Attachments:
1. Analysis of Proposed Operating License Change
 2. Proposed PNPS Operating License Changes (mark-up)
 3. Revised PNPS Operating License Pages
 4. Revised Cyber Security Plan Implementation Schedule
 5. List of Regulatory Commitments

cc: Mr. Daniel H. Dorman
Regional Administrator, Region I
U.S. Nuclear Regulatory Commission
2100 Renaissance Boulevard, Suite 100
King of Prussia, PA 19406-1415

U. S. Nuclear Regulatory Commission
ATTN: Director, Office of Nuclear Reactor Regulation
One White Flint North
11555 Rockville Pike
Rockville, MD 20852

NRC Senior Resident Inspector
Pilgrim Nuclear Power Station

Mr. Richard V. Guzman, Senior Project Manager
Office of Nuclear Reactor Regulation
U.S. Nuclear Regulatory Commission
Mail Stop O-8C2A
Washington, DC 20555

Mr. John Giarrusso Jr.
Planning, Nuclear & Preparedness Section Chief
Mass. Emergency Management Agency
400 Worcester Road
Framingham, MA 01702

Attachment 1

PNPS Letter 2.15.045

Analysis of Proposed Operating License Change

1.0 SUMMARY DESCRIPTION

This license amendment request (LAR) includes a proposed change to the Pilgrim Nuclear Power Station (PNPS) Cyber Security Plan (CSP) Implementation Schedule Milestone 8 full implementation date and a proposed revision to the existing operating license Physical Protection license condition.

2.0 DETAILED DESCRIPTION

In Reference 1, the NRC provided criteria to be used for evaluation of a license amendment request to revise the Cyber Security Implementation Schedule Milestone 8 date. In Reference 2, the NRC issued license amendments that approved the PNPS CSP and associated implementation milestone schedule. The CSP Implementation Schedule approved by Reference 2 was utilized as a portion of the basis for the NRC's safety evaluation report provided in Reference 2. In Reference 3, the NRC issued license amendments that approved a revised implementation milestone schedule. Entergy Nuclear Operations, Inc. (Entergy) is proposing a change to the Milestone 8 date from June 30, 2016, to December 15, 2017, for full implementation of the CSP for all applicable safety, security, and emergency preparedness (SSEP) functions.

3.0 TECHNICAL EVALUATION

In November 2009, in accordance with 10 CFR 73.54 (nuclear cyber security rule), each Entergy licensee submitted a proposed schedule for achieving full compliance with the rule. The schedule was approved (Reference 2) and consists of eight milestones, with interim Milestones 1 through 7 being completed by December 31, 2012, and Milestone 8 (full compliance) to be completed by December 15, 2014. During the process of accomplishing Interim Milestones 1 through 7 and commencing Milestone 8 work, it became evident to Entergy that additional time would be required, and a schedule extension request to June 30, 2016, was approved by the NRC (Reference 3). However, it has subsequently become evident that an additional extension is necessary. The extension requested herein is for a Milestone 8 date of December 15, 2017.

Below is Entergy's discussion of the eight evaluation criteria provided by Reference 1.

1. Identification of the specific requirement or requirements of the CSP that the licensee needs additional time to implement.

The CSP Sections 3 and 4 describe requirements for application and maintenance of cyber security controls listed in Nuclear Energy Institute (NEI) 08-09, Revision 6, *Cyber Security Plan for Nuclear power Reactors*, Appendices D and E. Application of the controls is accomplished after completion of detailed analyses (the cyber security assessment process) that identify "gaps," or the difference between current configuration and a configuration that satisfies each cyber security control. Gap closure can require any combination of physical, logical (software-related), or programmatic/procedural changes.

2. Detailed justification that describes the reason additional time is required to implement the specific requirement or requirements identified.

- a. Entergy hosted a "pilot" Milestone 8 inspection at the Indian Point site in March 2014. During the pilot, insight was gained into NRC interpretation on how to apply the cyber security controls listed in NEI 08-09, Revision 6. These interpretations were not previously available. During the pilot inspection, the NRC team reviewed several examples of critical digital assets (CDAs) with Entergy and indicated the level of detail and depth expected for the technical analyses against cyber security controls referenced in NEI 08-09. Based on this review, it is evident to Entergy that the detail and depth of the technical analysis exceeds Entergy's prior understanding and requires a considerably greater effort to achieve than initially anticipated.
- b. During 2015, each operating Entergy licensee has an inspection of compliance with interim Milestones 1 through 7. The preparation for and support of these inspections has required a significant commitment of time from Entergy's most knowledgeable subject matter experts on nuclear cyber security, exceeding the estimate previously developed and therefore, drawing those resources away from Milestone 8 implementation activities.
- c. Development of an endorsed written standard for interpreting and applying the NEI 08-09 cyber security controls have continued to be a work-in-progress over the past five years. NEI 13-10, Revision 2, a guideline intended to provide some reduction of controls implementation based on equipment safety significance, has been endorsed. However, an initial screening of Entergy CDAs using this guideline indicates the reduction in both analytical work and actual application of controls would not be significant.
- d. In June 2014, NEI submitted a petition for rulemaking to the Commission. The petition was subsequently found acceptable for review. The petition proposes a change to the rule to more precisely align the scope of the rule with the underlying objective of preventing radiological sabotage, which NEI estimates could potentially result in a reduction in the scope of cyber security implementation. While Entergy does not intend to suspend any implementation work in anticipation of the petition being approved, the petition being submitted is indicative that the final process for implementing the rule has not stabilized, and therefore, Entergy requires additional time to receive any implementation benefit from such rulemaking.
- e. Benchmarking data gathered on Milestone 8 implementation schedules for non-Entergy licensees indicates that a significant number of licensees have either gained approval for a new Milestone 8 date or submitted an extension request significantly beyond Entergy's current due date; therefore, Entergy's request is consistent with the industry.

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

The proposed completion date for Milestone 8 is December 15, 2017.

4. Evaluation of the impact that the additional time to implement the requirements will have on the effectiveness of the overall cyber security program in the context of milestones already completed.

The impact of the requested additional implementation time on the effectiveness of the overall cyber security program is considered to be very low, because the Interim Milestones already completed have resulted in a high degree of protection of safety-related, important-to-safety, and security CDAs against threat vectors associated with external connectivity (both wired and wireless), and portable digital media and devices. Additionally, extensive physical and administrative measures are already in place for CDAs pursuant to the PNPS Security Plan and Technical Specification requirements. In the context of cyber security milestones already completed, the following is noted:

- a. An Entergy Cyber Security Assessment Team (CSAT) has been implemented consisting of highly experienced personnel knowledgeable in reactor and balance-of-plant design, licensing, safety, security, emergency preparedness, information technology, and cyber security. The CSAT is provided with the authority, via written procedure, to perform the analyses and oversight activities described in the CSP. Entergy employs a single overall fleet-wide CSAT to ensure consistency of results among the fleet.
- b. Critical systems and CDAs have been identified, documented, and entered in a controlled database.
- c. The plant process computer network and the plant security computer network have been deterministically isolated per the requirements of cyber security Interim Milestone 3.
- d. Safety-related, important-to-safety, and security CDAs have been extensively reviewed and verified (or modified) to be deterministically isolated and not to employ wireless network technology.
- e. Procedures have been implemented for portable digital media and devices periodically connected to CDAs, per NEI 08-09, Revision 6, Appendix D, Section 1.19.
- f. CDAs associated with physical security target sets have been analyzed per the requirements of the CSP Section 3.1.6 and either (1) verified to satisfy the Technical Cyber Security Controls described in NEI 08-09, Revision 6, Appendix D or (2) actions required to satisfy the Technical Cyber Security Controls described in NEI 08-09, Revision 6, Appendix D, are captured in the Corrective Action Program (CAP).
- g. Employees have been provided with training on cyber security awareness, tampering, and control of portable digital media and devices periodically connected to CDAs.

- h. Entergy has transitioned from the previous cyber security program described by NEI 04-04. Revisions have been made to procedures that control plant modifications, planning, and maintenance, establishing ties to cyber security procedures for CDA analysis and control of portable digital media and devices periodically connected to CDAs.

5. Description of the methodology for prioritizing completion of work for CDAs associated with significant SSEP consequences and with reactivity effects in the balance of plant.

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). Further, in regard to deterministic isolation and control of portable media devices (PMD) for safety-related, important-to-safety (including BOP), and security CDAs, maintenance of one-way or air-gapped configurations and implementation of control of PMD remains high priority. This prioritization enabled completion of cyber security Interim Milestones 3 and 4. 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. Discussion of the cyber security program performance up to the date of the license amendment request.

No compromise of SSEP function by cyber means has been identified. Additionally, a Quality Assurance (QA) audit was conducted in the fourth quarter of 2014 pursuant to the physical security program review required by 10 CFR 73.55(m). The QA audit included review of cyber security program implementation. There were no significant findings related to overall cyber security program performance and effectiveness.

7. Discussion of cyber security issues pending in the CAP.

No significant (with 'significant' meaning constituting a threat to a CDA via cyber means or calling into question program effectiveness) nuclear cyber security issues are currently pending in the CAP. Several non-significant issues identified during the QA audit described above and identified during NRC inspections of compliance with nuclear cyber security Interim Milestones 1 through 7 have been entered into CAP. In addition, when the Reference 4 internal NRC memorandum was shared with Entergy, the actions described regarding cyber security Interim Milestone 4 were entered into CAP for evaluation by the CSAT.

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

Modifications completed include those required to deterministically isolate the Level 3 and 4 CDAs, as required by Interim Milestone 3, by data diode or air gap.

Potential modifications not yet implemented include automated security information event monitoring systems for monitoring activity on networks of CDAs, pursuant to NEI 08-09, Revision 6, Appendix D-2 (Audit and Accountability), and Appendices E-3.4 (Monitoring Tools and Techniques), 3.5 (Security Alerts and Advisories), and 4.3 (Personnel Performing maintenance and Testing Activities), and additional physical controls for CDAs outside the Protected Area pursuant to NEI 08-09, Revision 6, Appendix E-5.1 (Physical and Operational Environment Protection Policies and Procedures).

This LAR includes the proposed change to the existing operating license condition for "Physical Protection" (Attachments 2 and 3) for PNPS. This LAR also contains the proposed Revised CSP Implementation Schedule (Attachment 4) and provides a revised list of regulatory commitments (Attachment 5).

4.0 REGULATORY EVALUATION

4.1 Applicable Regulatory Requirements/Criteria

10 CFR 73.54 requires licensees to maintain and implement a Cyber Security Plan (CSP). Pilgrim Nuclear Power Station (PNPS) Facility Operating License Number DPR-35, includes a Physical Protection license condition that requires Entergy 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).

4.2 Significant Safety Hazards Consideration

Entergy is requesting an amendment to the PNPS Facility Operating License to revise the Physical Protection license condition as it relates to the CSP. This change includes a proposed change to a CSP Implementation Schedule milestone date and a proposed revision to the PNPS Facility Operating License to include the proposed deviation. Specifically, Entergy is proposing a change to the Implementation Milestone 8 completion date.

Entergy 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 change involve a significant increase in the probability or consequences of an accident previously evaluated?
Response: No.

The proposed change to the CSP Implementation Schedule is administrative in nature. This change 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 have 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 CSP Implementation Schedule is administrative in nature. This proposed change 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 do 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 for operation, limiting safety system settings, and safety limits specified in the technical specifications. The proposed change to the CSP Implementation Schedule is administrative in nature. In addition, the milestone date delay for full implementation of the CSP has no substantive impact because other measures have been taken which provide adequate protection during this period of time. Because there is no change to established safety margins as a 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, Entergy 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.

4.3 Conclusion

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 provides a change to the CSP 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 the amendment.

6.0 REFERENCES

1. NRC Internal Memorandum to Barry Westreich from Russell Felts, *Review Criteria for 10 CFR 73.54, Cyber Security Implementation Schedule Milestone 8 License Amendment Requests*, dated October 24, 2013 (ML13295A467)
2. NRC letter to Entergy, *Issuance of Amendment Re: Approval of CSP*, dated July 22, 2011, PNPS Letter 1.11.048 (ML11152A043)
3. NRC letter to Entergy, *Issuance of Amendment Re: Cyber Security Implementation Schedule Revision*, dated December 11, 2014, PNPS Letter 1.14.083, (ML14336A661)
4. NRC internal memorandum from the Director Cyber Security Directorate, Office of Nuclear Security and Incident Response, to the Region I through IV Directors of Reactor Safety, *Enhanced Guidance for Licensee Near-Term Corrective Actions to Address Cyber Security Inspection Findings and Licensee Eligibility for "Good-Faith" Attempt Discretion, Enclosure 2, Milestone 4 Resolution Actions*, dated July 1, 2013 (ML13178A203)

Attachment 2

PNPS Letter 2.15.045

Proposed PNPS Operating License Changes (mark-up)

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. **243**, 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, and 241, and **XXX**.

Attachment 3

PNPS Letter 2.15.045

Revised PNPS Operating License Pages

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. , 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 .

Attachment 4

PNPS Letter 2.15.045

Revised Cyber Security Plan Implementation Schedule

Revised Cyber Security Plan Implementation Schedule

| # | Implementation Milestone | Completion Date | Basis |
|---|---|-----------------|---|
| 8 | Full implementation of Pilgrim Nuclear Power Station (PNPS) Cyber Security Plan for all safety, security, and emergency preparedness (SSEP) functions will be achieved. | Dec. 15, 2017 | By the completion date, the PNPS 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. |

Attachment 5

PNPS Letter 2.15.045

List of Regulatory Commitments

List of Regulatory Commitments

The following table identifies those actions committed to by Entergy in this document. Any other statements in this submittal are provided for information purposes and are not considered to be regulatory commitments.

| COMMITMENT | TYPE (Check One) | | SCHEDULED COMPLETION DATE (If Required) |
|---|--------------------|--------------------------|--|
| | ONE-TIME ACTION | CONTINUING COMPLIANCE | |
| Full implementation of Pilgrim Nuclear Power Station Cyber Security Plan for all safety, security, and emergency preparedness functions will be achieved. | X | | Dec. 15, 2017 |