Entergy

Entergy Nuclear Operations, Inc.
Palisades Nuclear Plant
27780 Blue Star Memorial Highway
Covert, MI 49043-9530
Tel 269-764-2000

Anthony J. Vitale
Site Vice President

PNP 2015-035

June 11, 2015

U. S. Nuclear Regulatory Commission
ATTN: Document Control Desk
Washington, DC 20555-0001

SUBJECT: License Amendment Request – Cyber Security Plan Implementation Schedule

Palisades Nuclear Plant
Docket 50-255
Renewed Facility Operating License No. DPR-20

REFERENCES:

1. NRC Internal Memorandum to Barry Westreich from Russell Felts, *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)

2. NRC letter to Entergy Nuclear Operations, Inc., *Palisades Nuclear Plant - Issuance of Amendment Regarding the Cyber Security Plan: (TAC No . ME4355),* dated July 28, 2011 (ADAMS Accession No. ML111801243)

3. NRC letter to Entergy Nuclear Operations, Inc., *Palisades Nuclear Plant - Issuance of Amendment Re: Cyber Security Plan Implementation Schedule (TAC No. MF3303)*, dated December 8, 2014 (ADAMS Accession No. ML14237A144)

Dear Sir or Madam:

Pursuant to 10 CFR 50.4 and 10 CFR 50.90, Entergy Nuclear Operations, Inc. (ENO) hereby requests an amendment to the Renewed Facility Operating Licenses for Palisades Nuclear Plant (PNP). In accordance with the guidelines provided by Reference 1, this request proposes a change to the PNP 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 analysis of the proposed change. Attachment 2 contains proposed marked-up operating license pages for the Physical Protection license condition for PNP that reference the commitment change provided in this submittal. Attachment 3 contains the proposed revised operating license pages. Attachment 4 contains a revised Cyber Security Plan Implementation Schedule which includes a change to the completion date for Implementation Milestone 8. Attachment 5 contains one revised commitment related to the full implementation of PNP Cyber Security Plan.

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.

ENO requests approval of the proposed license amendment by June 30, 2016. Once approved, the amendment will be effective as of the date of issuance and shall be implemented within 30 days.

This letter contains one revised commitment related to the full implementation of PNP Cyber Security Plan, which is listed in Attachment 5.

In accordance with 10 CFR 50.91(b), ENO is notifying the State of Michigan of this proposed license amendment by transmitting a copy of this letter to the designated state official.

Should you have any questions concerning this letter, or require additional information, please contact Jim Miksa at 269-764-2945.

I declare under penalty of perjury that the foregoing is true and correct. Executed on June 11, 2015.

Sincerely,

ajv/jpm

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

cc: Administrator, Region III, USNRC
Project Manager, Palisades, USNRC
Resident Inspector, Palisades, USNRC
State of Michigan

ATTACHMENT 1

ANALYSIS OF PROPOSED OPERATING LICENSE CHANGE

Seven pages follow

ATTACHMENT 1
ANALYSIS OF PROPOSED OPERATING LICENSE CHANGE

1.0 SUMMARY DESCRIPTION

This license amendment request (LAR) includes a proposed change to the Palisades Nuclear Plant (PNP) 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 Nuclear Regulatory Commission (NRC) issued a license amendment to the Renewed Facility Operating License for PNP that approved the PNP 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 a license amendment that approved a revised implementation milestone schedule. Entergy Nuclear Operations, Inc. (ENO) 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 ENO 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 completing Interim Milestones 1 through 7 and commencing Milestone 8 work, it became evident to ENO 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 request is necessary. The extension requested herein is for a Milestone 8 date of December 15, 2017.

Below is ENO's discussion of the eight evaluation criteria provided in 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 (i.e., 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. ENO hosted a "pilot" Milestone 8 inspection at the Indian Point Energy Center in March 2014. During the pilot, insight was gained into the Nuclear Regulatory Commission's (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 with ENO several examples of critical digital assets (CDAs), describing the level of detail and depth expected in the technical analyses for cyber security controls referenced in NEI 08-09. Based on this review, it is evident to ENO that the detail and depth of the technical analysis exceeds ENO's prior understanding and requires a considerably greater effort to achieve than initially anticipated.

b. During 2015, each operating ENO 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 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.

c. Development of an endorsed written standard for interpreting and implementing the NEI 08-09 cyber security controls has continued to be a work-in-progress over the past five years. NEI 13-10, *Cyber Security Control Assessments*, Revision 2, a guideline intended to provide some reduction of controls implementation based on equipment safety significance, has been endorsed by the NRC. However, an initial screening of ENO's CDAs using this guideline indicates that 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 NRC. The petition was subsequently found acceptable for review. The petition proposes a change to 10 CFR 73.54, 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 ENO does not intend to suspend any implementation work in anticipation of the petition being approved, the petition being submitted is indicative that the process for implementing the rule is not finalized, and ENO needs additional time to receive any implementation benefit from such rulemaking.

e. Benchmarking data gathered on Milestone 8 implementation schedules for non-ENO licensees indicates that a significant number of them have either gained approval for a new Milestone 8 date or submitted an extension request significantly beyond ENO's current due date; therefore, ENO'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 that have already been 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 because they are plant components, pursuant to the PNP Physical Security Plan and Technical Specification requirements. In the context of cyber security milestones already completed, the following is noted:

a. An ENO 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. ENO 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 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 devices periodically connected to CDAs.

h. ENO has transitioned from the previous cyber security program described in 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 a 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), *Requirements for Physical Protection of Licensed Activities in Nuclear Power Reactors Against Radiological Sabotage; Security Program Reviews.* 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 corrective action program.

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 the CAP. Additionally, when the Reference 4 internal NRC memorandum was shared with ENO, the actions described regarding cyber security Interim Milestone 4 were entered into the 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 PNP. 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 CSP. PNP's Renewed Facility Operating License No. DPR-20 includes a Physical Protection license condition that requires ENO to fully implement and maintain in effect all provisions of the NRC 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 Nuclear Operations, Inc. (ENO) is requesting an amendment to the Palisades Nuclear Plant (PNP) Facility Renewed Operating License to revise the Physical Protection license condition as it relates to the Cyber Security Plan (CSP). This change includes a proposed change to a CSP implementation schedule milestone date and a proposed revision to the PNP Operating License to include the proposed deviation. Specifically, ENO is proposing a change to the Implementation Milestone 8 completion date.

ENO 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 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 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 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 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, ENO 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 (ADAMS Accession No. ML13295A467)

2. NRC letter to ENO, *Palisades Nuclear Plant - Issuance of Amendment Regarding Cyber Security Plan: (TAC NO. ME4355)*, dated July 28, 2011 (ADAMS Accession No. ML111801243)

3. NRC letter to Entergy Nuclear Operations, Inc., *Palisades Nuclear Plant – Issuance of Amendment RE: Cyber Security Plan Implementation Schedule (TAC No. MF3303)*, dated December 8, 2014 (ADAMS Accession No. ML14237A144)

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, d*ated July 1, 2013 (ADAMS Accession No. ML13178A203)

ATTACHMENT 2

Proposed PNP Operating License Changes
(showing proposed changes; additions are highlighted and deletions are strikethrough)

One page follows

D. The facility has been granted certain exemptions from Appendix J to 10 CFR Part 50, "Primary Reactor Containment Leakage Testing for Water Cooled Power Reactors." This section contains leakage test requirements, schedules and acceptance criteria for tests of the leak-tight integrity of the primary reactor containment and systems and components which penetrate the containment. These exemptions were granted in a letter dated December 6, 1989.

These exemptions granted pursuant to 10 CFR 50.12, are authorized by law, will not present an undue risk to the public health and safety, and are consistent with the common defense and security. With these exemptions, the facility will operate, to the extent authorized herein, in conformity with the application, as amended, the provisions of the Act, and the rules and regulations of the Commission.

E. ENO 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 contains Safeguards Information protected under 10 CFR 73.21, is entitled: "Entergy Nuclear Palisades Nuclear Plant Physical Security Plan."

ENO 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 Palisades CSP was approved by License Amendment No. 243 as supplemented by changes approved by License Amendment Nos. 248, ~~and~~ 253, and XXX.

F. [deleted]

G. ENP and ENO shall have and maintain financial protection of such type and in such amounts as the Commission shall require in accordance with Section 170 of the Atomic Energy Act of 1954, as amended, to cover public liability claims.

ATTACHMENT 3

Operating License Page Change Instructions

and

Revised PNP Operating License Pages

Two pages follow

Page Change Instructions

ATTACHMENT TO LICENSE AMENDMENT NO. 2XX

RENEWED FACILITY OPERATING LICENSE NO. DPR-20

DOCKET NO. 50-255

Remove the following page of Renewed Facility Operating License, and replace with the attached revised page. The revised page is identified by amendment number and contains a line in the margin indicating the area of change.

REMOVE	INSERT
Page 6	Page 6

D. The facility has been granted certain exemptions from Appendix J to 10 CFR Part 50, "Primary Reactor Containment Leakage Testing for Water Cooled Power Reactors." This section contains leakage test requirements, schedules and acceptance criteria for tests of the leak-tight integrity of the primary reactor containment and systems and components which penetrate the containment. These exemptions were granted in a letter dated December 6, 1989.

These exemptions granted pursuant to 10 CFR 50.12, are authorized by law, will not present an undue risk to the public health and safety, and are consistent with the common defense and security. With these exemptions, the facility will operate, to the extent authorized herein, in conformity with the application, as amended, the provisions of the Act, and the rules and regulations of the Commission.

E. ENO 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 contains Safeguards Information protected under 10 CFR 73.21, is entitled: "Entergy Nuclear Palisades Nuclear Plant Physical Security Plan."

ENO 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 Palisades CSP was approved by License Amendment No. 243 as supplemented by changes approved by License Amendment Nos. 248, 253, and XXX.

F. [deleted]

G. ENP and ENO shall have and maintain financial protection of such type and in such amounts as the Commission shall require in accordance with Section 170 of the Atomic Energy Act of 1954, as amended, to cover public liability claims.

ATTACHMENT 4

REVISED CYBER SECURITY PLAN IMPLEMENTATION SCHEDULE

One page follows

ATTACHMENT 4

Revised Cyber Security Plan Implementation Schedule

#	Implementation Milestone	Completion Date	Basis
8	Full implementation of *Palisades Nuclear Plant (PNP) Cyber Security Plan* for all safety, security, and emergency preparedness (SSEP) functions will be achieved.	December 15, 2017	By the completion date, the PNP 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

LIST OF REGULATORY COMMITMENTS

One page follows

ATTACHMENT 5

List of Regulatory Commitments

The following table identifies those actions committed to by Entergy Nuclear Operations, Inc. 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 *Palisades Nuclear Plant Cyber Security Plan* for all safety, security, and emergency preparedness functions will be achieved.	X		December 15, 2017