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

December 8, 2014

Vice President, Operations
Entergy Nuclear Operations, Inc.
Palisades Nuclear Plant
27780 Blue Star Memorial Highway
Covert, MI 49043-9530

SUBJECT: PALISADES NUCLEAR PLANT - ISSUANCE OF AMENDMENT RE: CYBER SECURITY PLAN IMPLEMENTATION SCHEDULE (TAC NO. MF3303)

Dear Sir or Madam:

The U.S. Nuclear Regulatory Commission (NRC) has issued the enclosed Amendment No. 253 to Renewed Facility Operating License No. DPR-20 for the Palisades Nuclear Plant (PNP). The amendment consists of changes to the facility operating license in response to your application dated December 30, 2013, as supplemented by letter dated May 22, 2014.

The amendment approves the revised schedule for full implementation of the cyber security plan (CSP) and revises Paragraph 2.E of Renewed Facility Operating License No. DPR-20 for PNP, to incorporate the revised CSP implementation schedule.

A copy of our related safety evaluation is also enclosed. The Notice of Issuance will be included in the Commission's biweekly *Federal Register* notice.

Sincerely,

Jennivine K. Rankin, Project Manager
Plant Licensing Branch III-1
Division of Operating Reactor Licensing
Office of Nuclear Reactor Regulation

Docket No. 50-255

Enclosures:
1. Amendment No. 253 to DPR-20
2. Safety Evaluation

cc: Distribution via ListServ

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

ENTERGY NUCLEAR OPERATIONS, INC.

DOCKET NO. 50-255

PALISADES NUCLEAR PLANT

AMENDMENT TO RENEWED FACILITY OPERATING LICENSE

Amendment No. 253
Renewed Facility Operating License No. DPR-20

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

   A. The application for amendment by Entergy Nuclear Operations, Inc. (the licensee), dated December 30, 2013, as supplemented by letter dated May 22, 2014, complies with the standards and requirements of the Atomic Energy Act of 1954, as amended (the Act), and the Commission's rules and regulations set forth in 10 CFR Chapter I;

   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;

   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 as indicated in the attachment to this license amendment, and Paragraph 2.E of Renewed Facility Operating License No. DPR-20 is hereby amended to read as follows:

> 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.

3. 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 December 30, 2013, 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

David L. Pelton, Chief
Plant Licensing Branch III-1
Division of Operating Reactor Licensing
Office of Nuclear Reactor Regulation

Attachment:
Changes to the Renewed Facility
Operating License No. DPR-20

Date of Issuance: December 8, 2014

ATTACHMENT TO LICENSE AMENDMENT NO. 253

RENEWED FACILITY OPERATING LICENSE NO. DPR-20

DOCKET NO. 50-255

Replace the following page of the Renewed Facility Operating License No. DPR-20 with the attached revised page. The changed area is identified by a marginal line.

REMOVE	INSERT
Page 6	Page 6

D. The facility has been granted certain exemptions from the requirements of Section III, G of Appendix R to 10 CFR Part 50, "Fire Protection Program for Nuclear Power Facilities Operating Prior to January 1, 1979." This section relates to fire protection features for ensuring the systems and associated circuits used to achieve and maintain safe shutdown are free of fire damage. These exemptions were granted in letters dated February 8, 1983, July 12, 1985, and July 23, 1985.

In addition, 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.

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.

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

SAFETY EVALUATION BY THE OFFICE OF NUCLEAR REACTOR REGULATION

RELATED TO AMENDMENT NO. 253 TO

RENEWED FACILITY OPERATING LICENSE NO. DPR-20

ENTERGY NUCLEAR OPERATIONS, INC.

PALISADES NUCLEAR PLANT

DOCKET NO. 50-255

1.0 INTRODUCTION

By letter dated December 30, 2013 (Agencywide Documents Access and Management System (ADAMS) Accession No. ML13364A328), as supplemented by letter dated May 22, 2014 (ADAMS Accession No. ML14142A296), Entergy Nuclear Operations, Inc. (ENO, the licensee) requested a change to the renewed facility operating license for Palisades Nuclear Plant (PNP).

The proposed change would revise the date of Cyber Security Plan (CSP) Implementation Schedule Milestone 8 and Paragraph 2.E in the renewed facility operating license. Milestone 8 of the CSP implementation schedule concerns the full implementation of the CSP. Portions of the letter dated December 30, 2013, contain sensitive unclassified non-safeguards (security-related) information and, accordingly, those portions are withheld from public disclosure.

The supplement dated May 22, 2014, provided additional information that clarified the application, did not expand the scope of the application as originally noticed, and did not change the U.S. Nuclear Regulatory Commission (NRC or the Commission) staff's original proposed no significant hazards consideration determination as published in the *Federal Register* on April 15, 2014 (79 FR 21297).

2.0 REGULATORY EVALUATION

The NRC staff reviewed and approved the licensee's existing CSP implementation schedule for PNP by letter dated July 28, 2011, Amendment No. 243 (ADAMS Accession No. ML111801243), concurrent with the incorporation of the CSP into the facility's current licensing basis. 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.

- Review criteria provided by the NRC staff's internal 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), to be considered for evaluating 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, "[i]mplementation 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.

3.0 TECHNICAL EVALUATION

3.1 Licensee's Requested Change

The NRC staff issued Amendment No. 243 to Renewed Facility Operating License DPR-20 for PNP by letter dated July 28, 2011. This amendment approved the CSP and associated implementation schedule, and added a license condition requiring the licensee to fully implement and maintain the Commission-approved CSP. The 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 Cyber Security Program 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 PNP CSP requires the licensee to fully implement the CSP by December 15, 2014. By letter dated December 30, 2013, the licensee proposed to modify the Milestone 8 completion date to June 30, 2016.

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 requirements of the CSP that needed additional time to implement are Section 3, "Analyzing Digital Computer Systems and Networks" and Section 4, "Establishing, Implementing and Maintaining the Cyber Security Program." It further noted that these sections describe requirements for application and maintenance of cyber security controls and described the process of addressing security controls. The licensee described specific requirements needing additional time including determining the need for a specific security features to provide for audit and accountability; monitoring tools and techniques; analyzing security alerts and advisories; and to assist personnel performing maintenance and testing activities. It also described a need for additional physical security controls for CDAs outside the security protected area and significant programmatic change management associated with approximately 40 procedure revisions related to operational and management cyber 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 the following:

> ENO is using a robust full-time team of approximately 20 personnel to perform and document the detailed analysis (cyber security assessment process)... However, even with that level of resource commitment, the analysis, which began in 2011, [was] projected to be completed by the second quarter of 2014.
>
> Since the number of CDAs and existing procedures is in the hundreds and the

> number of individual cyber security control attributes is also in the hundreds the total of physical, logical and programmatic changes required constitutes a significant project involving plant components and systems and substantial planning. Additionally, changes to CDAs and procedures must be integrated into the plant operational schedule including on-line operations, maintenance and testing, as well as planning and execution of refueling outages. With this analysis [scheduled to conclude in the second quarter of 2014, it was] expected that insufficient time will remain in 2014 to conduct modification and change management planning activities and execution.

Planning for implementation of CSP Sections 3 and 4, as discussed in Section 1 above is expected to occur in 2014 and be implemented in the following 18 months.

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 June 30, 2016, and stated the revised Milestone 8 date will provide a six month contingency for the security features mentioned in Item 1 above. The revised completion date allows the necessary time to fully integrate cyber controls into the plant processes, provide all the necessary training and change management, and reinforce behavior changes of the entire organization around nuclear cyber security.

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 stated the following:

> 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 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, extensive physical and administrative measures are already in place for CDAs because they are plant components, pursuant to the Physical Security Plan and Technical Specification Requirements.

The licensee then provided a detailed list of cyber security milestones already completed. The NRC staff was concerned the LAR did not address all seven milestones and provided a request for additional information (RAI) to the licensee by email dated April 30, 2014 (ADAMS Accession No. ML14121A017). The licensee responded by letter May 22, 2014 (ADAMS Accession No. ML14142A296). The licensee's response indicated that the milestone of concern had been implemented and the extension would have no effect on the milestones mentioned in the response.

5. A description of the licensee's methodology for prioritizing completion of work for critical digital assets associated with significant safety consequences and with reactivity effects in the balance of plant.

The licensee stated its methodology for prioritizing CDA activities is centered on considerations for safety, security, and emergency preparedness (SSEP) and BOP (continuity of power) consequences. The licensee stated the following:

> 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.
>
> This prioritization enabled completion of cyber security Interim Milestones 3 and 4 in 2012. 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 that there has been no identified compromise of SSEP functions by cyber means at any ENO plant. PNP Milestone 1 through 7 actions were successfully completed by December 31, 2012. These actions provide a high degree of protection against cyber attacks while full program actions are in progress. The licensee also noted a formal Quality Assurance audit in the last quarter of 2013 that included review of the CSP implementation and that there were no significant findings related to overall cyber security program performance and effectiveness.

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

The licensee stated the following:

> There are presently no significant nuclear cyber security issues pending in the Corrective Action Program (CAP) that constitute a threat to a CDA via cyber means or calling into question program effectiveness. Several non-significant issues identified during the Quality Assurance audit described above have been entered into CAP. Additionally, when the Reference 3 internal NRC memorandum was shared with ENO, the actions described regarding cyber security Interim Milestone 4 were entered into CAP for evaluation by the CSAT. Final actions regarding some program activities are pending.

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

The licensee discussed completed modifications 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's staff's evaluation is below. The NRC staff finds that the actions the licensee noted as being required to implement 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 concludes 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. Therefore, the NRC has reasonable assurance that full implementation of the CSP by June 30, 2016 will provide adequate protection of the public health and safety and the common defense and security.

The licensee has stated that the scope of actions and resources required to fully implement its CSP were not anticipated when the implementation schedule was originally determined. The NRC staff recognizes that CDA assessment work to include application of controls is much more complex and resource intensive than originally anticipated, in part due to the NRC expanding the scope of the cyber security requirements to include balance of plant. As a result, the licensee has a large number of additional tasks not originally considered when developing its CSP implementation schedule. The NRC staff concludes that the licensee's request for additional time to implement Milestone 8 is reasonable given the unanticipated complexity, volume, and scope of the remaining work required to fully implement its CSP.

The licensee proposed a Milestone 8 completion date of June 30, 2016. The licensee stated that changing the completion date of Milestone 8 allows for the application of changes to CDAs, procedures and cyber security controls and provides the necessary time to methodically plan, implement, and test the required additions or changes and allows those additions or changes that require a design change to be performed. The licensee stated its methodology for prioritizing Milestone 8 activities is centered on considerations for SSEP and BOP (continuity of power) consequences. The methodology is based on defense–in–depth, installed configuration of the CDA and susceptibility to commonly identified threat vectors. Prioritization for CDA assessment begins with safety related CDAs and continues through lower priority non-safety and EP CDAs. The NRC staff concludes that based on the large number of digital assets described above and the limited resources with the appropriate expertise to perform these activities, the licensee's methodology for prioritizing work on CDAs is appropriate. The staff further concludes that the licensee's request to delay final implementation of the CSP until June 30, 2016, is reasonable given the complexity of the remaining unanticipated work.

3.3 Technical Evaluation Conclusion

The NRC staff concludes that the licensee's request to delay full implementation of its CSP until June 30, 2016, 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 much more complicated than anticipated and not reasonably foreseeable when the CSP implementation schedule was originally developed; and (iii) the licensee has reasonably prioritized and scheduled the work required to come into full compliance with its CSP implementation schedule.

3.4 Revision to License Condition 2.E

By letter dated December 30, 2013, the licensee proposed to modify Paragraph 2.E of Renewed Facility Operating License No. DPR-20 for PNP, 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 2.E of Renewed Facility Operating License No. DPR-20 for PNP states, in part:

> 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 a change approved by License Amendment No. 248).

The revised license condition in Paragraph 2.E of Renewed Facility Operating License No. DPR-20 for PNP would state:

> 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.

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

4.0 REGULATORY COMMITMENTS

By letter dated December 30, 2013, the licensee made the following regulatory commitment:

> Full implementation of Palisades Nuclear Plant Cyber Security Plan for all safety, security, and emergency preparedness functions will be achieved.
>
> Scheduled Completion Date: June 30, 2016

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

5.0 STATE CONSULTATION

In accordance with the Commission's regulations, the Michigan State official was notified of the proposed issuance of the amendment. The Michigan State official had no comments.

6.0 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 cyber security plan 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.

7.0 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/CSD

Date: December 8, 2014

A copy of our related safety evaluation is also enclosed. The Notice of Issuance will be included in the Commission's biweekly *Federal Register* notice.

Sincerely,

/RA/

Jennivine K. Rankin, Project Manager
Plant Licensing Branch III-1
Division of Operating Reactor Licensing
Office of Nuclear Reactor Regulation

Docket No. 50-255

Enclosures:
1. Amendment No. 253 to DPR-20
2. Safety Evaluation

cc: Distribution via ListServ

DISTRIBUTION:
PUBLIC
LPL3-1 Reading
RidsAcrsAcnw_MailCTR Resource
RidsNrrDorlDpr Resource
RidsNrrDorlLpl3-1 Resource
RidsNrrPMPalisades Resource
RidsNrrLAMHenderson Resource
RidsRgn3MailCenter Resource
RidsNsirCsd Resource
JRycyna, NSIR/CSD

ADAMS Accession No.: ML14237A144 ***by email**

OFFICE	NRR/DORL/LPL3-1/PM	NRR/DORL/LPL3-1/LA	NSIR/CSD/D
NAME	JRankin	MHenderson	RFelts
DATE	11/10/2014	11/10/2014	11/10/2014
OFFICE	OGC *	NRR/DORL/LPL3-1/BC	NRR/DORL/LPL3-1/PM
NAME	NStamour w/edits	DPelton	JRankin
DATE	12/4/2014	12/08/2014	12/08/2014

OFFICIAL AGENCY RECORD