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

December 15, 2017

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 (CAC NO. MF9523; EPID L-2017-LLA-0199)

Dear Sir or Madam:

The U.S. Nuclear Regulatory Commission has issued the enclosed Amendment No. 264 to Renewed Facility Operating License No. DPR-20 for the Palisades Nuclear Plant (PNP). The amendment changes the Cyber Security Plan (CSP) Milestone 8 full implementation date in response to your application dated March 30, 2017, as supplemented by letter dated October 17, 2017.

The amendment revises the CSP Milestone 8 full implementation date by extending the date from December 15, 2017, to March 31, 2019. The amendment also revises Paragraph 2.E of the Renewed Facility Operating License No. DPR-20 for PNP, to incorporate the revised CSP implementation schedule.

A copy of the 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
Division of Operating Reactor Licensing
Office of Nuclear Reactor Regulation

Docket No. 50-255

Enclosures:
1. Amendment No. 264 to DPR-20
2. Safety Evaluation

cc: 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. 264
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. (ENO, or the licensee), dated March 30, 2017, as supplemented by letter dated October 17, 2017, 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 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, 259, and 264.

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 October 17, 2017, 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 J. Wrona, Chief
Plant Licensing Branch III
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 15, 2017

ATTACHMENT TO LICENSE AMENDMENT NO. 264

PALISADES NUCLEAR PLANT

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 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, 259, and 264.

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. 264 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 March 30, 2017 (Agencywide Documents Access and Management System (ADAMS) Accession No. ML17089A380), as supplemented by letter dated October 17, 2017 (ADAMS Accession No. ML17290A342), Entergy Nuclear Operations, Inc. (ENO, the licensee) requested a change to the renewed facility operating license (RFOL) for Palisades Nuclear Plant (PNP).

On March 30, 2017, the licensee submitted a request to revise the date of the Cyber Security Plan (CSP) implementation schedule Milestone 8 and Paragraph 2.E in the RFOL from December 15, 2017, to May 31, 2020. Milestone 8 of the CSP implementation schedule concerns the full implementation of the CSP. The basis for this change was to support PNP's transition from an operating power plant to a decommissioned plant, starting on October 1, 2018. By letter dated September 28, 2017 (ADAMS Accession No. ML17271A233), as supplemented by letter dated October 19, 2017 (ADAMS Accession No. ML17292A032), the licensee informed the U.S. Nuclear Regulatory Commission (NRC or Commission) that it has decided to cease power operations at PNP no later than May 31, 2022, instead of on October 1, 2018. As a result of the new cessation date, the licensee supplemented their license amendment request by letter dated October 17, 2017. This supplement requested to revise the date of the CSP implementation schedule Milestone 8 and Paragraph 2.E in the RFOL from December 15, 2017, to March 31, 2019.

The NRC staff initially reviewed and approved the licensee's CSP implementation schedule for PNP by License Amendment No. 243, dated July 28, 2011 (ADAMS Accession No. ML111801243), to RFOL DPR-20 concurrent with the incorporation of the CSP into the facility's current licensing basis. The NRC staff reviewed and approved the licensee's current CSP implementation schedule by License Amendment No. 259, dated May 2, 2016 (ADAMS Accession No. ML16078A068). License Amendment No. 259 required the licensee to fully implement and maintain all provisions of the CSP no later than December 15, 2017.

On May 23, 2017, the NRC staff published a proposed no significant hazards consideration (NSHC) determination in the *Federal Register* (82 FR 23623) for the proposed amendment.

Subsequently, by letter dated October 17, 2017, the licensee provided additional information that expanded the scope of the amendment request as originally noticed in the *Federal Register*. Accordingly, the NRC published a second proposed NSHC determination in the *Federal Register* on November 7, 2017 (82 FR 51650), which superseded the original notice in its entirety.

2.0 REGULATORY EVALUATION

The NRC staff considered the following regulatory requirements and guidance in its review of the license amendment request 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 RFOL 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, in part, that "[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 pursuant to 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 License Amendment No. 243 to RFOL No. DPR-20 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 CSP identified completion dates and bases for the following eight milestones:

1) Establish the cyber security assessment team;

2) Identify critical systems 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; and

8) Fully implement the CSP.

Currently, Milestone 8 of the PNP CSP requires the licensee to fully implement the CSP by December 15, 2017. By letter dated October 17, 2017, the licensee proposed to modify the Milestone 8 completion date to March 31, 2019.

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 requested that full implementation of the CSP requirements per Milestone 8 be rescheduled from December 15, 2017, to March 31, 2019. The specific requirement is described in Cyber Security Plan, Section 3.1, "Analyzing Digital Computer Systems and Networks and Applying Cyber Security Controls." The licensee said during the additional period ENO will continue to comply with the requirements of Milestones 1 through 7.

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

   The licensee stated that on January 4, 2017, it notified the NRC of its intent to permanently cease operations at PNP effective October 1, 2018. After this notification, PNP continued to maintain the previously implemented Milestones 1-7 actions, but suspended work toward achieving Milestone 8. In September 2017, ENO stated it decided to continue operating PNP until the spring of 2022.

Additional time is required to achieve Milestone 8 because of (1) the time lost while work was suspended between December 2016 and the September 2017 ENO announcement to continue PNP operation until 2022, (2) the time required to prepare new IT staff prior to starting CSP Milestone 8 assessments to ensure a quality product, (3) the time required to identify and implement modifications, if any, during the planned PNP fall 2018 refueling outage, and (4) the time required to complete CSP Milestone 8 assessments after the 2018 refueling outage.

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

The licensee stated that the proposed completion date for Milestone 8 is March 31, 2019.

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 that cyber security protections provided by the completion and maintenance of Milestone 1 through 7 actions ensure that the program will continue to be effective in mitigating the risk of the design basis threat via cyber means. The licensee states that safety-related, important-to-safety, and security CDAs will continue to be deterministically isolated from external networks; stringent control of portable media and mobile devices connected to CDAs will continue, and implementation of technical cyber security controls and security officer observation for CDAs that support physical security target set functions will also continue. Although, it is not required until Milestone 8, the licensee is in the process of implementing procedures governing CDA configuration management, cyber security incident response and recovery, and cyber security training.

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

The licensee said CDAs are plant components that are subject to the maintenance prioritization and normal work management process. The licensee says this places the highest priority on apparent conditions adverse to quality in system, structure, and component (SSC) design function and factors such as safety risk, nuclear defense-in-depth, and continuity of electric power generation in the balance-of-plant (BOP). In regard to deterministic isolation and control of portable media and mobile devices for safety-related, important-to-safety (including BOP), and security CDAs, maintenance of one-way or air gapped configurations and implementation of controls of portable media and mobile devices remain a high priority. This prioritization enabled timely completion of Milestones 3 and 4. Additionally, the licensee says it continues to give prompt attention to any emergent issue with CDAs that would potentially challenge the established cyber protective barriers.

6) Discussion of the cyber security program performance up to the date of the LAR.

The licensee stated that no compromise of SSEP functions by cyber means has been identified. ENO said an NRC inspections of its compliance with Milestones 1 through 7 was completed on September 17, 2015 and findings from the inspection were designated as having a very low safety significance (green non-cited, granted enforcement discretion). The follow-up inspection completed December 31, 2016, and documented in inspection report dated February 14, 2017 (ADAMS Accession No. ML17045A709), reviewed the licensee's corrective actions resulting from the 2015 inspection and did not identify any additional findings.

Additionally, at PNP an annual ENO quality assurance audit has been conducted every year since 2013 pursuant to the requirements of 10 CFR 73.55(m), "Security program reviews." The licensee stated there have been no significant audit findings related to the overall cyber security program performance and effectiveness during these audits.

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

The licensee stated that there are no cyber security issues that would constitute a threat to proper CDA function or that would call into question cyber security program effectiveness are currently pending in the CAP.

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

The licensee stated that modifications completed include those required to deterministically isolate Level 3 and 4 CDAs, as required by nuclear cyber security implementation schedule interim Milestone 3. Additionally, the licensee said no modifications are pending.

3.2 NRC Staff Evaluation of Requested Change

As stated in Section 2.0 of this safety evaluation, changes to the NRC-approved CSP implementation schedule require NRC approval pursuant to 10 CFR 50.90. The NRC staff has evaluated the licensee's application using the regulatory requirements and NRC guidance set forth above. The NRC staff finds that the licensee's basis for requesting an extension to the Milestone 8 implementation date and the proposed timetable to achieve full compliance is reasonable, as discussed in the staff evaluation below.

The licensee indicated that the activities associated with the CSP, as described in Milestones 1 through 7, were completed prior to December 31, 2012. The licensee also indicated that during the proposed extension period ENO will continue to comply with the requirements of Milestones 1 through 7.

The NRC notes that the licensee has implemented Milestones 1-7, as documented in inspection reports dated October 14, 2015, and February 14, 2017 (ADAMS Accession Nos. ML15289A409 and ML17045A709, respectively). The NRC staff concludes that successful implementation of Milestones 1-7 provide a high degree of protection to ensure that the most significant digital computer and communication system and networks associated with SSEP functions are sufficiently protected against cyber attacks. In addition, the NRC staff concludes

that the licensee established a reasonable methodology for prioritizing completion of work for CDAs associated with SSEP consequences and with reactivity effects in the BOP. This framework is sufficient because it allows the licensee to promptly address any emergent CDA issues that would challenge cyber security measures in the interim, while the licensee completes all Milestone 8 activities.

In addition, the licensee is in progress of implementing certain aspects of Milestone 8, including (1) CDA configuration management, (2) cyber security incident response and recovery, and (3) cyber security training. Other cyber security measures have been implemented such as maintenance prioritization and normal work management processes that place priority on conditions adverse to quality in SSC design function, as well as threats to continuity of electric power generation in the BOP, and prompt attention to any emergent issue with CDAs that would potentially challenge the established cyber protective barriers. Collectively, these measures provide adequate protection of the public health and safety and common defense and security.

The licensee initially notified the NRC that it would permanently cease operations at PNP on October 1, 2018. After ENO's December 2016 announcement to permanently cease operations at PNP in October 2018, work on completing CSP Milestone 8 activities was suspended. As such, the licensee did not perform the Milestone 8 work scheduled for their spring 2017 refueling outage. Recently, however, the licensee decided to continue operating PNP until the spring of 2022. This resulted in the licensee submitting a new certification of permanent power cessation for PNP to the NRC on September 28, 2017. The suspension of Milestone 8 activities from December 2016 to September 2017, while ENO prepared for facility closure, as well as the refueling outage scheduled for fall 2018, have added time to the CSP implementation schedule. Accordingly, ENO has requested a change to the Milestone 8 full implementation date from December 15, 2017, to March 31, 2019.

The licensee requested an extension date of March 31, 2019, in part, because Milestone 8 work will need to be performed in the next refueling outage (fall 2018). In addition, the licensee also stated that time is required to complete CSP Milestone 8 assessments after the 2018 refueling outage. The NRC staff notes the circumstance at PNP were unanticipated as PNP was expected to cease power operations in October 2018. The decision to continue to operate past the original cessation date is not a normal practice. The NRC staff has determined that implementation of any necessary Milestone 8 changes to safety, emergency planning, and BOP systems, are activities which need to be undertaken during a shutdown. Accordingly, ENO's plan to conduct these activities within the next year (i.e., fall 2018) is reasonable.

The NRC staff also finds that the additional amount of time following the fall 2018 refueling outage is reasonable to perform assessments, finalize the programmatic changes to the cyber security program, and provide cyber protection to BOP systems. For the reasons described above, the NRC staff finds the circumstances at PNP are sufficient to justify an extension of the CSP implementation schedule until March 31, 2019. The staff concludes the completion of initial Milestone 8 activities and ENO's commitment to fully implement the cyber security rule and PNP's CSP provide assurance that 10 CFR 73.54 will be met. Therefore, the NRC has reasonable assurance that full implementation of the CSP by March 31, 2019, will provide adequate protection of the public health and safety and the common defense and security. The NRC staff finds the proposed change acceptable.

3.3 Technical Evaluation Conclusion

The NRC staff finds that the licensee's request to delay the full implementation of its CSP until

March 31, 2019, is reasonable; therefore, the staff grants the amendment. The bases for the staff's determination are: (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, and (ii) additional time to fully comply with the CSP implementation schedule is needed due to unanticipated circumstances that arose at PNP.

3.4 Revision to License Condition 2.E

The license is amended by changes to paragraph 2.E of RFOL No. DPR-20.

By letter dated March 30, 2017, as supplemented by letter dated October 17, 2017, the licensee proposed to modify Paragraph 2.E of RFOL 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 RFOL 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 changes approved by License Amendment Nos. 248, 253, and 259.

The revised portion of the license condition in paragraph 2.E of RFOL 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, 253, 259, and 264.

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 FINAL NO SIGNIFICANT HAZARDS CONSIDERATION

The NRC's regulations in 10 CFR 50.92 state that the NRC may make a final determination, under the procedures in 10 CFR 50.91, that a license amendment involves no significant hazards consideration if operation of the facility, in accordance with the amendment, would not: (1) involve a significant increase in the probability or consequences of an accident previously evaluated; or (2) create the possibility of a new or different kind of accident from any accident previously evaluated; or (3) involve a significant reduction in a margin of safety.

As required by 10 CFR 50.91(a), an evaluation of the issue of no significant hazards consideration is presented 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, system, 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.

5.0 REGULATORY COMMITMENTS

By letter dated October 17, 2017, the licensee made the following regulatory commitment:

> Full implementation of *Palisades Nuclear Plant (PNP) Cyber Security Plan* for all safety, security, and emergency preparedness (SSEP) functions will be achieved.
>
> Scheduled Completion Date: March 31, 2019

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

6.0 STATE CONSULTATION

In accordance with the Commission's regulations, the Michigan State official was notified of the proposed issuance of the amendment on November 21, 2017. The Michigan State official had no comments.

7.0 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. The Commission has previously issued a proposed finding that the amendment involves no significant hazards consideration, and there has been no public comment on such finding published in the *Federal Register* on November 7, 2017 (82 FR 51650). 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.

8.0 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: S. Coker, NSIR/CSD

Date of issuance: December 15, 2017

SUBJECT: PALISADES NUCLEAR PLANT - ISSUANCE OF AMENDMENT RE: CYBER SECURITY PLAN IMPLEMENTATION SCHEDULE (CAC NO. MF9523; EPID L-2017-LLA-0199) DATED DECEMBER 15, 2017

DISTRIBUTION:
PUBLIC
RidsAcrs_MailCTR Resource
RidsNrrDorlDpr Resource
RidsNrrDorlLpl3 Resource
RidsNrrPMPalisades Resource
RidsRgn3MailCenter Resource
RidsNrrLASRohrer Resource
RidsNsirCsd Resource
SCoker, NSIR/CSD

ADAMS Accession No. ML17328B033 ***via email**

OFFICE	NRR/DORL/LPL3/PM	NRR/DORL/LPL3/LA	NSIR/DPCP/CSD/BC*
NAME	JRankin	SRohrer	JBeardsley
DATE	11/28/2017	11/28/2017	12/11/17
OFFICE	OGC - NLO subject to counsel provided by EMAIL dated 12/12/2017	NRR/DORL/LPL3/BC	NRR/DORL/LPL3/PM
NAME	PJehle	DWrona	JRankin
DATE	12/13/2017	12/14/2017	12/15/2017

OFFICIAL AGENCY RECORD