NRR-PMDAPEm Resource

From: ERICKSON, JEFFREY S [JERICKS@entergy.com]
Sent: Thursday, August 21, 2014 7:57 AM
To: Rankin, Jennivine
Cc: Hardy, Jeffery A; MIKSA, JAMES P
Subject: RE: Draft Safety Evaluation for LAR for Approval of Revised Cyber Security Plan Implementation Schedule (TAC No MF3303)
Attachments: Draft SE for SR review.docx

Jennie,

Palisades agrees with the NRC staff's determination that none of the information contained in the attached draft SE for the cyber security implementation schedule license amendment request is security-related information.

Thanks,

Jeff Erickson
Palisades Regulatory Assurance

From: Rankin, Jennivine [mailto:Jennivine.Rankin@nrc.gov]
Sent: Wednesday, August 20, 2014 9:10 PM
To: ERICKSON, JEFFREY S
Subject: Draft Safety Evaluation for LAR for Approval of Revised Cyber Security Plan Implementation Schedule (TAC No MF3303)

Jeff,

Please see the attached copy of the Draft Safety Evaluation (SE) for the subject License Amendment Request. The information in section 3.3 of the Draft SE as well as the Milestone 8 implementation date was identified as security-related information in your application dated December 30, 2013 (Agencywide Documents Access and Management System (ADAMS) Accession No. ML13364A328). The NRC staff does not consider this information to be security-related and the information is likely to be included in the final staff SE which will be publically available. Please review the Draft SE and confirm by e-mail that you agree with the NRC staff's determination and none of the information contained in the attached Draft SE is security-related information.

Thanks,
Jennie

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

Hearing Identifier: NRR_PMDA
Email Number: 1524

Mail Envelope Properties (AACFD50AA516704FAADD585E032049170AB6D726)

Subject: RE: Draft Safety Evaluation for LAR for Approval of Revised Cyber Security Plan Implementation Schedule (TAC No MF3303)
Sent Date: 8/21/2014 7:57:20 AM
Received Date: 8/21/2014 7:57:23 AM
From: ERICKSON, JEFFREY S

Created By: JERICKS@entergy.com

Recipients:
"Hardy, Jeffery A" <jhardy@entergy.com>
Tracking Status: None
"MIKSA, JAMES P" <jmiksa@entergy.com>
Tracking Status: None
"Rankin, Jennivine" <Jennivine.Rankin@nrc.gov>
Tracking Status: None

Post Office: JDCXMETSP001.etrsouth.corp.entergy.com

Files	**Size**	**Date & Time**
MESSAGE	1534	8/21/2014 7:57:23 AM
Draft SE for SR review.docx	28873	

Options
Priority: Standard
Return Notification: No
Reply Requested: No
Sensitivity: Normal
Expiration Date:
Recipients Received:

DRAFT SAFETY EVALUATION BY THE OFFICE OF NUCLEAR REACTOR REGULATION

RELATED TO AMENDMENT NO. 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 NRC 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 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. By letter dated December 30, 2013, the licensee requested to change Milestone 8 of the CSP implementation schedule. 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).

3.0 TECHNICAL EVALUATION

3.1 Background

The NRC staff issued Amendment No. 243 to Renewed Facility Operation License DPR-20 for PNP by letter dated July 28, 2011. This amendment approved the CSP and associated implementation schedule. 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) Implement Installation of a deterministic one-way device 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) Commence ongoing monitoring and assessment activities for those target set CDAs whose security controls have been implemented;

8) Full implementation of the CSP for all safety, security and emergency preparedness functions.

3.2 Licensee's Proposed Change

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 has proposed to modify

Paragraph 2.E of renewed facility operation license DPR-20 for PNP to reflect the revised full implementation schedule for the CSP.

3.3 NRC Staff Evaluation

The licensee request dated December 30, 2013, is consistent with the NRC staff guidance dated October 24, 2013, developed to evaluate requests to postpone Milestone 8 implementation dates, and addressed the criteria stated in the guidance. The intent of the cyber security implementation schedule was for licensees to demonstrate ongoing implementation of their cyber security program prior to full implementation, which is set for the date specified in Milestone 8. Activities include establishing a CSAT, identifying critical systems and CDAs, installing deterministic one-way devices between defensive levels, implementing access control for portable and mobile devices, implementing methods to observe and identify obvious cyber related tampering, and conducting ongoing monitoring and assessment activities for target set CDAs. In their aggregate, the interim milestones demonstrate ongoing implementation of the cyber security program.

The criteria stated in the guidance document dated October 24, 2013, and addressed by the licensee as justification for the LAR are:

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

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

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

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.

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

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

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

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

The NRC staff evaluated the licensee's request based on the review criteria specified in the guidance document dated October 24, 2013. The NRC staff's evaluation is below, numbered as the criteria are above.

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 it 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 controls for CDAs outside the security protected area and significant programmatic change management associated with approximately 40 procedure changes related to operational and management cyber security controls.

The NRC staff agrees that implementation of CSP Sections 3 and 4 requires the extensive actions as described by the licensee and therefore requires additional time for full implementation of the CSP.

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

By letter dated December 30, 2013, 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 is presently 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 concluding in the second quarter of 2014, it is expected that insufficient time will remain in 2014 to conduct modification and change management planning activities and execution.
>
> Planning [for the specific security feature mentioned in Section 1 above] is expected to occur in 2014 and implement it in the following 18 months.

The NRC staff acknowledges implementation issues with large numbers of CDAs and the need to address many security control attributes for each. Based on the information provided by the licensee, the NRC staff concludes that the licensee has justified the need for additional time for fully implementing the requirements of the cyber security program described above.

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 feature mentioned in Section 1 above.

The NRC staff recognizes that delaying final implementation of the cyber security program will provide a contingency as well as time for the cyber security assessment follow-on work to be finished.

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.

By letter dated December 30, 2013, 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 also briefly described how the various milestones were implemented.

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 request had no effect on the milestones mentioned in the response.

The NRC staff concludes the impact of the requested additional implementation time on the effectiveness of the overall cyber security program is low. PNP is much more secure after implementing the milestones because the controls the licensee put in place mitigate the most significant cyber attack vectors on the most significant CDAs.

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.

By letter dated December 30, 2013, 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. Further, in regard to deterministic isolation and control of portable media devices (PMD) for safety-related, important-to-safety (including balance-of-plant) 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 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.

The NRC staff concludes the licensee's methodology is appropriate and conservative; therefore, acceptable to the NRC staff.

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

By letter dated December 30, 2013, the licensee stated that there has been no identified compromise of SSEP functions by cyber means at any ENO plant. The licensee noted its experience with the scanning of portable devices. The licensee also noted a formal Quality Assurance (QA) audit in the last quarter of 2013 that included review of the cyber security program implementation and that there were no significant findings related to overall cyber security program performance and effectiveness.

The NRC staff agrees that activities including the portable media/mobile computing device program and as well as other activities discussed above provide significant protection against cyber attacks. Based on the information provided by the licnesee, the NRC staff concludes that the licensee is using the quality tools at its disposal to verify the effectiveness of the cyber security program.

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

By letter dated December 30, 2013, 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.

The NRC staff concludes that the licensee is using its corrective action program to track issues for the cyber security program.

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

By letter dated December 30, 2013, the licensee discussed completed modifications and pending modifications. The NRC staff concluded that the discussions provided by the licensee describing modifications completed to support the cyber security program and pending cyber security modifications is consistent with the information provided in section 3.4 of this SE.