INDIANA MICHIGAN POWER®
A unit of American Electric Power

Indiana Michigan Power
Cook Nuclear Plant
One Cook Place
Bridgman, MI 49106
IndianaMichiganPower.com

May 27, 2014

AEP-NRC-2014-41
10 CFR 50.90
10 CFR 50.4

Docket Nos.: 50-315
50-316

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

Donald C. Cook Nuclear Plant Units 1 and 2
Response to Request for Additional Information Regarding the License Amendment Request to Revise the Cyber Security Plan Implementation Schedule

References:

1. Letter from J. P. Gebbie, Indiana Michigan Power Company (I&M), to U. S. Nuclear Regulatory Commission (NRC) Document Control Desk, "Donald C. Cook Nuclear Plant Units 1 and 2 License Amendment Request to Revise the Cyber Security Implementation Schedule," dated January 10, 2014, ADAMS Accession No. ML14015A142.
2. Letter from NRC to I&M, "Donald C. Cook Nuclear Plant, Units 1 and 2 - Request for Additional Information Concerning the Application for Amendment to Revise the Cyber Security Plan Implementation Schedule (Tac Nos. MF3363 and MF3364)," dated April 29, 2014, ADAMS Accession No. ML14113A305.

This letter provides Indiana Michigan Power Company's (I&M), licensee for Donald C. Cook Nuclear Plant (CNP) Units 1 and 2, response to the request for additional information (RAI) from the U. S. Nuclear Regulatory Commission (NRC) regarding the license amendment request (LAR) to revise the Cyber Security Plan (CSP) Implementation Schedule.

By Reference 1, I&M proposed to amend CNP Units 1 and 2 Renewed Facility Operating Licenses DPR-58 and DPR-74 to revise the full implementation date of the CNP CSP. By Reference 2, the NRC transmitted an RAI regarding the LAR submitted by I&M in Reference 1.

Enclosure 1 to this letter provides an affirmation statement pertaining to the information contained herein. Enclosure 2 provides I&M's response to the RAI.

Copies of this letter and its enclosures are being transmitted to the Michigan Public Service Commission and Michigan Department of Environmental Quality, in accordance with the requirements of 10 CFR 50.91.

S001A
NRR

There are no new regulatory commitments made in this letter. Should you have any questions, please contact Mr. Michael K. Scarpello, Regulatory Affairs Manager, at (269) 466-2649.

Sincerely,

Joel P. Gebbie
Site Vice President

TLC/amp

Enclosures:
1. Affirmation
2. Response to Request for Additional Information Regarding the License Amendment Request to Revise the Cyber Security Plan Implementation Schedule

c: J. T. King, MPSC
MDEQ-RMD/RPS
NRC Resident Inspector
C. D. Pederson, NRC Region III
T. J. Wengert, NRC Washington, DC
A. J. Williamson, AEP Ft. Wayne, w/o enclosures

Enclosure 1 to AEP-NRC-2014-41

AFFIRMATION

I, Joel P. Gebbie, being duly sworn, state that I am Site Vice President of Indiana Michigan Power Company (I&M), that I am authorized to sign and file this request with the U. S. Nuclear Regulatory Commission on behalf of I&M, and that the statements made and the matters set forth herein pertaining to I&M are true and correct to the best of my knowledge, information, and belief.

Indiana Michigan Power Company

Joel P. Gebbie
Site Vice President

SWORN TO AND SUBSCRIBED BEFORE ME

THIS 27 DAY OF May, 2014

Notary Public

My Commission Expires 04-04-2018

DANIELLE BURGOYNE
Notary Public, State of Michigan
County of Berrien
My Commission Expires 04-04-2018
Acting in the County of Berrien

Enclosure 2 to AEP-NRC-2014-41

Response to Request for Additional Information Regarding the License Amendment Request to Revise the Cyber Security Plan Implementation Schedule

By letter to the U. S. Nuclear Regulatory Commission (NRC) dated January 10, 2014 (ADAMS Accession No. ML14015A142), Indiana Michigan Power Company (I&M) submitted a license amendment request (LAR) to revise Milestone 8 of the Cyber Security Plan (CSP) Implementation Schedule for the Donald C. Cook Nuclear Plant (CNP) Units 1 and 2. To complete its review, the NRC staff issued a request for additional information (RAI). This RAI requested a response within 30 days of the RAI. The information request is restated below and followed by the I&M response.

RAI:

> *The January 10, 2014, LAR provides details concerning the results of a Performance Assurance Audit and mentions other audits and similar activities. However, the details of the results of these other audits and activities are not provided in the LAR. Please provide additional details concerning the results of the corporate security audit, self-assessments, and peer nuclear plant evaluations identified in the LAR.*

Response to RAI

As stated in the LAR, CNP conducted a corporate security audit, a self-assessment, and a peer nuclear plant review in preparation for implementation of the cyber security program. Additional details about the results of these activities are provided below.

Corporate Security Audit

American Electric Power (AEP) Corporate Information Security contracted with Ernst & Young to perform an audit of the security posture of all AEP owned assets using the Electricity Subsector Cybersecurity Capability Maturity Model (ES-C2M2). This is a facilitated self-assessment of security controls implemented on the analyzed networks that was performed by collecting data from questionnaires sent to various corporate groups in the fourth quarter of 2012. The purpose of the corporate audit was to determine areas where controls have been implemented and areas that need additional work. The scope of the audit that covered CNP was divided between the business network and those components that were covered by the CSP under NRC regulations. The focus areas for both the business network and CSP portions of the audit included the following:

- Cyber
- Response
- Sharing
- Asset
- Risk
- Access
- Threat
- Situation
- Dependencies
- Workforce

After the data was collected and compiled, the results were reviewed in March 2013. The audit showed all areas as being at least partially implemented, while a few areas had been largely implemented. These results were consistent with expectations because the CSP for plant systems had implemented the security controls associated only with Milestones 1 through 7. Implementation of items associated with Milestone 8 of the CSP had not yet begun.

While the audit helped determine the overall cyber security posture of the corporate information technology infrastructure, it did not provide a specific analysis of NRC-regulated areas. From a corporate standpoint, this audit was treated as an information gathering activity so there were no remedial actions. In addition, because the audit did not utilize standards based on NRC regulations, no corrective actions were initiated at CNP.

Self-Assessment

A self-assessment of CSP Milestones 1 through 7 was performed in March 2013 and found that CNP has met the requirements of those milestones from the CSP Implementation Schedule.

The following strengths were identified:

- CNP has a dedicated cyber security assessment team (CSAT), as opposed to several peer plants, at which the CSAT is assembled only for scheduled meetings.
- The members of the CNP CSAT and the Expert Cyber Security Target Set Panel are members of the Critical Group.

The self-assessment resulted in three recommendations:

- Ensure a process exists to address the replacement of CSAT members in a timely manner.
- An action request (AR) had recently been entered into the corrective action program that identified a condition in which the cyber security team did not have a process in place to track the expiration of cyber security software installed on laptops used on plant equipment. Corrective actions were identified but had not yet been in place long enough to verify effectiveness. Therefore, a recommendation was made to review the effectiveness of corrective actions during the next self-assessment.
- Develop a process to support the full Cyber Security Program implementation with respect to technical controls in the event that we add target set critical digital assets (CDA).

No nuclear safety or human performance issues were identified.

Actions Identified:

- Procedure PMP-5047-CSP-006, "Cyber Security Assessment Team," was revised to address CSAT membership.
- AR 2012-15260, "Severon Laptop Computer Expiration Date for Cyber Security," will be evaluated during the next self-assessment to determine the effectiveness of corrective actions

- A cyber security specification was developed for vendors who provide equipment that falls under the Cyber Security Program.

Peer Nuclear Plant Review

This peer review was performed in September 2013 by Utilities Service Alliance peers and determined that CNP has not completed the documentation necessary to demonstrate compliance with interim cyber security Milestones 1, 2, and 6. The review also identified that Milestone 4 actions associated with the July 1, 2013, enforcement discretion "good faith" letter have yet to be completed. Because no CDAs have been identified at CNP, Milestone 7 was not reviewed.

Actions Identified:

- Revise the CSAT procedure to address concerns with CSAT training (Milestone 1)
- Provide justification for the criteria that determines why a digital asset is a CDA (Milestone 2)
- Create a list of all locations for scanning kiosks (Milestone 2)
- Address concerns with tracking components associated with Target Set CDAs (Milestone 6)

The actions identified above were completed December 26, 2013.