



**INDIANA  
MICHIGAN  
POWER**

A unit of American Electric Power

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

July 19, 2010

AEP-NRC-2010-49  
10 CFR 50.90  
10 CFR 73.54

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

**SUBJECT:** Donald C. Cook Nuclear Plant Units 1 and 2  
Docket Nos. 50-315 and 50-316  
License Amendment Request for Approval of the Donald C. Cook Nuclear Plant  
Cyber Security Plan

Dear Sir or Madam:

By letter dated November 20, 2009, Indiana Michigan Power Company (I&M), the licensee for Donald C. Cook Nuclear Plant (CNP), submitted a request for an amendment to the Renewed Facility Operating Licenses (FOL) for CNP Unit 1 and Unit 2. This proposed amendment requested NRC approval of the CNP Cyber Security Plan, an implementation schedule for the Cyber Security Plan, and an addition to the existing FOL Physical Protection license condition requiring I&M to fully implement and maintain in effect all provisions of the approved Cyber Security Plan. By letter dated May 20, 2010, the NRC acknowledged receipt of I&M's letter and requested I&M to respond with either a revised submittal that addresses previously identified generic issues from use of NEI 08-09, Revision 3, or to respond by withdrawing the existing application and resubmitting a revised Cyber Security Plan consistent with Regulatory Guide 5.71 or NEI 08-09, Revision 6. In response to the NRC's request, I&M is withdrawing its previously submitted license amendment request dated November 20, 2009. Therefore, I&M is submitting a new license amendment request for approval of the CNP Cyber Security Plan consistent with NEI 08-09, Revision 6.

By letter dated April 28, 2010, the Nuclear Energy Institute (NEI) provided the Nuclear Regulatory Commission (NRC) a copy of NEI 08-09, "Cyber Security Plan for Nuclear Power Reactors," Revision 6, dated April 2010, for review and endorsement. By letter dated May 5, 2010, from the NRC to NEI, the NRC endorsed the use of NEI 08-09, Revision 6, as acceptable for use by licensees to comply with the requirements of 10 CFR 73.54 with the exception of the definition of "cyber attack." NEI responded with a new, proposed definition of "cyber attack" in a letter to the NRC, dated June 2, 2010. By letter dated June 7, 2010, from the NRC to NEI, the NRC accepted NEI's proposed definition for "cyber attack" and authorized licensees to incorporate this definition in cyber security plans based on NEI 08-09, Revision 6.

Enclosures 4 and 5 to this letter contain sensitive information  
Withhold from public disclosure under 10 CFR 2.390  
Upon removal of Enclosures 4 and 5, this letter is decontrolled

SECURITY-RELATED INFORMATION – WITHHOLD UNDER 10 CFR 2.390

5001A  
NRN

Pursuant to 10 CFR 50.90 and 10 CFR 73.54, Indiana Michigan Power Company, the licensee for CNP, is submitting a request for an amendment to the Renewed FOL for CNP Unit 1 and Unit 2. This proposed amendment requests NRC approval of the CNP Cyber Security Plan, an implementation schedule for the Cyber Security Plan, and an addition to the existing FOL Physical Protection license condition requiring I&M to fully implement and maintain in effect all provisions of the approved Cyber Security Plan.

Enclosure 1 to this letter provides an affirmation statement regarding the information in this letter. Enclosure 2 provides I&M's evaluation of the proposed change. Enclosure 3 provides the proposed implementation schedule required by 10 CFR 73.54 as regulatory commitments. Enclosure 4 provides the proposed CNP Cyber Security Plan which will be incorporated by reference into CNP's Physical Security Plan following NRC approval. Enclosure 5 provides the details of the deviations from NEI 08-09, Revision 6. Enclosure 6 to this letter provides the requested change to the FOL for CNP Unit 1 and Unit 2. Clean copies of the affected FOL pages with the proposed changes incorporated will be provided to the NRC Licensing Project Manager upon request. I&M requests that Enclosure 4 and Enclosure 5, which contain sensitive security related information, be withheld from public disclosure in accordance with 10 CFR 2.390.

I&M requests approval of the proposed amendment in accordance with the normal NRC review schedule. The proposed amendment will be implemented within 90 days of approval. The approved plan will be implemented in accordance with Enclosure 3.

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. This letter contains regulatory commitments.

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

AMD/jmr

Enclosures 4 and 5 to this letter contain sensitive information  
Withhold from public disclosure under 10 CFR 2.390  
Upon removal of Enclosures 4 and 5, this letter is decontrolled

SECURITY-RELATED INFORMATION – WITHHOLD UNDER 10 CFR 2.390

Enclosures:

1. Affirmation
2. Indiana Michigan Power Company's Evaluation
3. Implementation Schedule as Regulatory Commitments
4. Donald C. Cook Nuclear Plant Cyber Security Plan
5. Deviations from NEI 08-09, Revision 6
6. Proposed Facility Operating License Change

c: J. T. King, MPSC  
S. M. Krawec, AEP Ft. Wayne, w/o enclosures  
MDNRE – WHMD/RPS  
NRC Resident Inspector  
M. A. Satorius, NRC Region III  
P. S. Tam, NRC Washington DC

Enclosures 4 and 5 to this letter contain sensitive information  
Withhold from public disclosure under 10 CFR 2.390  
Upon removal of Enclosures 4 and 5, this letter is decontrolled

SECURITY-RELATED INFORMATION – WITHHOLD UNDER 10 CFR 2.390

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 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.

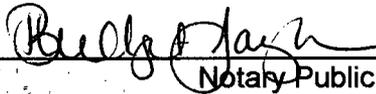
Indiana Michigan Power Company



Joel P. Gebbie  
Site Vice President

SWORN TO AND SUBSCRIBED BEFORE ME

THIS 15<sup>th</sup> DAY OF July, 2010

  
\_\_\_\_\_  
Notary Public

My Commission Expires 6/10/2013



Enclosure 2 to AEP-NRC-2010-49

INDIANA MICHIGAN POWER COMPANY'S EVALUATION

Subject: License Amendment Request for Approval of the Donald C. Cook Nuclear Plant  
Cyber Security Plan

1.0 DESCRIPTION

2.0 PROPOSED CHANGE

3.0 BACKGROUND

4.0 TECHNICAL ANALYSIS

5.0 REGULATORY SAFETY ANALYSIS

5.1 No Significant Hazards Consideration

5.2 Applicable Regulatory Requirements/Criteria

5.3 Conclusion

6.0 ENVIRONMENTAL CONSIDERATIONS

7.0 REFERENCES

## 1.0 DESCRIPTION

Pursuant to 10 CFR 50.90 and 10 CFR 73.54, Indiana Michigan Power Company (I&M), the licensee for Donald C. Cook Nuclear Plant (CNP), is submitting a request for an amendment to the Renewed Facility Operating Licenses (FOL) for CNP Unit 1 and Unit 2. This proposed amendment requests Nuclear Regulatory Commission (NRC) approval of the CNP Cyber Security Plan, an implementation schedule for the Cyber Security Plan, and addition to the existing FOL Physical Protection license condition requiring I&M to fully implement and maintain in effect all provisions of the approved Cyber Security Plan.

## 2.0 PROPOSED CHANGE

I&M proposes to implement the Donald C. Cook Nuclear Plant Cyber Security Plan, described in Enclosure 4 to this letter, in accordance with the implementation schedule described in Enclosure 3 to this letter.

I&M proposes to add a condition to the Unit 1 and the Unit 2 FOL, as described in Enclosure 6 to this letter. The proposed license condition will require that I&M implement and maintain in effect the Cyber Security Plan.

## 3.0 BACKGROUND

This license amendment request (LAR) consists of three parts: the proposed Cyber Security Plan, a proposed Implementation Schedule, and a proposed addition to the existing FOL Physical Protection license condition to require I&M to fully implement and maintain in effect all provisions of the Commission-approved cyber security plan as required by 10 CFR 73.54, "Protection of digital computer and communication systems and networks." The regulations in 10 CFR 73.54 establish the requirements for a cyber security program. These regulations require each licensee currently licensed to operate a nuclear power plant under 10 CFR 50 to submit a cyber security plan that satisfies the requirements of the rule. Each submittal must include a proposed implementation schedule and implementation of the licensee's cyber security program must be consistent with the approved schedule. The background for this application is addressed by the NRC Notice of Availability published on March 27, 2009, in Federal Register notice 74 FR 13926 (Reference 1).

## 4.0 TECHNICAL ANALYSIS

Reference 1 issued the final rule that amended 10 CFR Part 73. The cyber security requirements codified as 10 CFR 73.54 are designed to provide high assurance that digital computer and communication systems and networks are adequately protected against cyber attacks up to and including the design basis threat established by 10 CFR 73.1(a)(1)(v). These requirements are substantial improvements upon the requirements imposed by the NRC's Order Modifying License, EA-02-026 (Reference 2).

By letter dated April 28, 2010 (Reference 3), the Nuclear Energy Institute (NEI) provided NEI 08-09, Revision 6, to the NRC for review and endorsement. NEI 08-09, Revision 6, provides a template for use by licensees in development of their own cyber security plans.

This LAR includes the proposed plan (Enclosure 4) that conforms to the template provided in NEI 08-09 with deviations documented in Enclosure 5. In addition, the LAR includes the proposed change to the existing FOL license condition for "Physical Protection" (Enclosure 6). Finally, the LAR contains the proposed Implementation Schedule (Enclosure 3) as required by 10 CFR 73.54.

## 5.0 REGULATORY SAFETY ANALYSIS

### 5.1 Applicable Regulatory Requirements / Criteria

This LAR is submitted pursuant to 10 CFR 73.54 which requires licensees currently licensed to operate a nuclear power plant under 10 CFR Part 50 to submit a Cyber Security Plan in accordance with 10 CFR 50.4 and 50.90.

### 5.2 No Significant Hazards Consideration

I&M has evaluated whether 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 of occurrence or consequences of an accident previously evaluated?**

Response: No

The proposed change is required by 10 CFR 73.54 and includes three parts. The first part is the submittal of the Donald C. Cook Nuclear Plant (CNP) Cyber Security Plan for Nuclear Regulatory Commission (NRC) review and approval. The plan provides a description of how the requirements of the rule will be implemented at CNP. The plan establishes the licensing basis for the Indiana Michigan Power Company (I&M) Cyber Security Program for CNP. The plan establishes how to achieve high assurance that nuclear power plant digital computer and communication systems and networks associated with the following are adequately protected against cyber attacks up to and including the design basis threat:

1. Safety-related and important-to safety functions,
2. Security functions,
3. Emergency preparedness functions including offsite communications, and
4. Support systems and equipment which, if compromised, would adversely impact safety, security, or emergency preparedness functions.

The plan is designed to provide high assurance that the systems and networks are protected from cyber attacks. The plan, itself, does not require any plant modifications. However, implementation of the plan is expected to require plant configuration changes. The plan describes how plant modifications that involve digital computers and communication systems and networks will be reviewed to provide high assurance of adequate protection against cyber attacks, up to and including the design basis threat as defined in 10 CFR 73.54. Changes to the systems and networks will be evaluated per 10 CFR 50.59 to determine if a License Amendment is required. Changes to the systems and networks will be evaluated per 10 CFR 50.54(q) to determine if the effectiveness of the site Emergency Plan is reduced. Changes to the systems and networks will be evaluated per 10 CFR 50.54(p) to determine if the effectiveness of the site Security Plan is reduced. Prior NRC approval will be obtained if required by these evaluations.

The plan, itself, does not alter the plant configuration, require new plant equipment to be installed, alter accident analysis assumptions, add any initiators, or effect the function of plant systems or the manner in which systems are operated, maintained, modified, tested, or inspected. The plan has no impact on the probability or consequences of an accident previously evaluated.

The second part of the proposed change is an implementation schedule. The third part adds a sentence to the existing Renewed Facility Operating Licenses (FOL) license condition for physical protection. Both of these changes are administrative and have 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 first part of the proposed change is the submittal of the Cyber Security Plan for NRC review and approval. The plan provides a description of how the requirements of 10 CFR 73.54 will be implemented at CNP.

The plan does not require any plant modifications. The plan describes how plant modifications involving digital computer systems will be reviewed to provide high assurance of adequate protection against cyber attacks, up to and including the design basis threat defined in 10 CFR 73.54. The plan does not alter the plant configuration, require new plant equipment to be installed, 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 plan is designed to provide high assurance that the systems within the scope of the rule are protected from cyber attacks and does not create the possibility of a new or different kind of accident from any previously evaluated.

The second part of the proposed change is an implementation schedule. The third part adds a sentence to the existing FOL license condition for physical protection. Both of these

changes are administrative and do not create the possibility of a new or different kind of accident from any previously evaluated.

Therefore, the proposed change does not create the possibility of a new or different kind of accident from any previously evaluated.

**3. Does the proposed change involve a significant reduction in a margin of safety?**

Response: No

The first part of the proposed change is the submittal of the plan for NRC review and approval. The plan is designed to provide high assurance that the systems within the scope of the rule are protected from cyber attacks. Plant safety margins are established through Limiting Conditions for Operation, Limiting Safety System Settings, and Safety Limits specified in the Technical Specifications. Because there is no change to these established safety margins, the proposed change does not involve a significant reduction in a margin of safety.

The second part of the proposed change is an implementation schedule. The third part adds a sentence to the existing FOL license condition for physical protection. Both of these changes are administrative and do 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.

**5.3 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. I&M concludes that the proposed amendment 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.

## 6.0 ENVIRONMENTAL CONSIDERATIONS

A review has determined that the proposed amendment would change a requirement with respect to installation or use of a facility component located within the restricted area, as defined in 10 CFR 20, or would change an inspection or surveillance requirement. However, the proposed amendment does not involve (i) a significant hazards consideration, (ii) a significant change in the types of or significant increase in the amounts of any effluent that may be released offsite, or (iii) a significant increase in individual or cumulative occupational radiation exposure. Accordingly, the proposed amendment meets the eligibility criterion for 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 proposed amendment.

## 7.0 REFERENCES

1. Federal Register Notice, Final Rule 10 CFR Part 73, Power Reactor Security Requirements, published on March 27, 2009, 74 FR 13926.
2. EA-02-026, Order Modifying Licenses, Safeguards and Security Plan Requirements, issued February 25, 2002. (ADAMS Accession No. ML020500059)
3. Letter from J. W. Roe, Nuclear Energy Institute (NEI), to S. A. Morris, Nuclear Regulatory Commission (NRC), "NEI 08-09, Revision 6, Cyber Security Plan for Nuclear Power Reactors, April 2010," dated April 28, 2010. (ADAMS Accession No. ML101180434)

Enclosure 3 to AEP-NRC-2010-49

**DONALD C. COOK NUCLEAR PLANT CYBER SECURITY PLAN  
IMPLEMENTATION SCHEDULE**

**Donald C. Cook Nuclear Plant Cyber Security Plan  
Implementation Schedule as Regulatory Commitments**

The following table identifies those actions committed to by Indiana Michigan Power Company (I&M) for implementation of the Donald C. Cook Nuclear Plant (CNP) Cyber Security Plan. Any other actions discussed in this submittal represent intended or planned actions by I&M. They are described to the Nuclear Regulatory Commission (NRC) for the NRC's information and are not regulatory commitments.

<b>Commitment</b>	<b>Completion Date</b>
Train and qualify Cyber Security Assessment Team.	June 30, 2011
Identify Critical Systems and Critical Digital Assets.	June 30, 2011
Develop Cyber Security Defensive Strategy.	June 30, 2011
Implement cyber security defense-in-depth architecture for isolation boundaries.	June 30, 2012
Implement cyber security defense-in-depth architecture for all other non-isolation boundaries.	June 30, 2013
Establish Cyber Security Program policies/procedures.	December 31, 2013
Perform and document the cyber security assessment described in the Cyber Security Plan.	December 31, 2013
Implement Security Controls not requiring a plant modification.	48 months after NRC approval of Cyber Security Plan
The Cyber Security Program is implemented and the Program has entered maintenance phase.	48 months after NRC approval of Cyber Security Plan