



A unit of American Electric Power

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

April 8, 2011

AEP-NRC-2011-18  
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  
Response to Request for Information Regarding a License Amendment Request for Approval of the Donald C. Cook Nuclear Plant Cyber Security Plan (TAC Nos. ME4275 and ME4276)

Dear Sir or Madam:

By letter dated July 19, 2010, Indiana Michigan Power Company (I&M), the licensee for Donald C. Cook Nuclear Plant (CNP), submitted a license amendment request for approval of the CNP Cyber Security Plan (CSP) consistent with Nuclear Energy Institute (NEI) 08-09, Revision 6. By e-mail dated March 10, 2011, the Nuclear Regulatory Commission (NRC) communicated to CNP a request for additional information (RAI). This RAI required a response to three generic issues which involve a clarification on the scope of 10 CFR 73.54 with respect to Balance of Plant (BOP) systems, cyber security records retention, and the CSP implementation schedule. NEI and the Cyber Security Task Force have worked to develop resolution to these generic issues which are acceptable to the NRC staff.

By letter dated January 5, 2011, the NRC informed NEI of the preferred language for the CSP to address the BOP scope issue. By letter dated February 28, 2011, NEI submitted to the NRC, a proposed resolution to the records retention issue. The NRC response dated March 1, 2011, informed NEI that the proposed resolution is acceptable. By letter dated February 28, 2011, NEI submitted to the NRC, a template for implementation schedules. The NRC response dated March 1, 2011, informed NEI that the template is acceptable.

Enclosure 1 to this letter provides an affirmation statement regarding the information in this letter. Enclosure 2 provides I&M's response to the NRC RAI. Enclosure 3 provides a table of revised commitments. Enclosure 4 provides the proposed CNP CSP, which reflects changes discussed in Enclosure 2, which will be incorporated by reference into CNP's Physical Security Plan following NRC approval and replaces, in its entirety, the CNP CSP which was submitted to the NRC by letter dated July 19, 2010. I&M requests that Enclosure 4, which contains sensitive security related information, be withheld from public disclosure in accordance with 10 CFR 2.390.

Enclosure 4 to this letter contains sensitive information  
Withhold from public disclosure under 10 CFR 2.390  
Upon removal of Enclosure 4, this letter is decontrolled

SECURITY-RELATED INFORMATION – WITHHOLD UNDER 10 CFR 2.390

S001A

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.

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

DMB/jmr

Enclosures:

1. Affirmation
2. Response to NRC Request for Additional Information
3. Implementation Schedule as Regulatory Commitments
4. Donald C. Cook Nuclear Plant Cyber Security Plan

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

Enclosure 4 to this letter contains sensitive information  
Withhold from public disclosure under 10 CFR 2.390  
Upon removal of Enclosure 4, this letter is decontrolled

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.

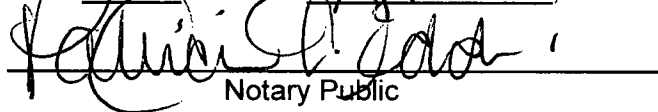
Indiana Michigan Power Company



Joel P. Gebbie  
Site Vice President

SWORN TO AND SUBSCRIBED BEFORE ME

THIS 5<sup>th</sup> DAY OF APRIL, 2011

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

My Commission Expires 11-5-2011

## Enclosure 2 to AEP-NRC-2011-18

### Response to NRC Request for Additional Information

By letter dated July 19, 2010, Indiana Michigan Power Company (I&M), the licensee for Donald C. Cook Nuclear Plant (CNP), submitted a license amendment request for approval of the CNP Cyber Security Plan (CSP) consistent with Nuclear Energy Institute (NEI) 08-09, Revision 6. By e-mail dated March 10, 2011, the Nuclear Regulatory Commission (NRC) communicated to CNP a request for additional information (RAI). This RAI required a response to three generic issues which involve a clarification on the scope of 10 CFR 73.54 with respect to Balance of Plant (BOP) systems, cyber security records retention, and the CSP implementation schedule. NEI and the Cyber Security Task Force have worked to develop resolution to these generic issues which are acceptable to the NRC staff. These resolutions provide a consistent industry position. Each RAI item is restated below followed by the corresponding I&M response.

#### **NRC RAI Question 1**

*Title 10 of the code of Federal Regulations (10 CFR) Paragraph 73.54(c)(2) requires licensees to design a cyber security program to ensure the capability to detect, respond to, and recover from cyber attacks. Furthermore, 10 CFR 73.54(e)(2)(i) requires licensees to maintain a cyber security plan that describes how the licensee will maintain the capability for timely detection and respond to cyber attacks. The ability for a licensee to detect and respond to cyber attacks requires accurate and complete records and is further supported by 10 CFR 73.54(h), which states that the licensee shall retain all records and supporting technical documentation required to satisfy the requirements of 10 CFR Section 73.54 as a record until the commission terminates the license for which the records were developed, and shall maintain superseded portions of these records for at least 3 years after the record is superseded, unless otherwise specified by the commission.*

*The licensee's Cyber Security Plan (CSP) in Section [4.13] states that Critical Digital Asset (CDA) audit records and audit data (e.g.; operating system logs, network device logs) are retained for a period of time that is less than what is required by 10 CFR 73.54(h).*

*Explain the deviation from the 10 CFR 73.54(h) requirement to retain records and supporting technical documentation until the commission terminates the license (or to maintain superseded portions of these records for at least 3 years) and how that meets the requirements of 10 CFR 73.54.*

#### **I&M Response**

I&M will replace the language in Section 4.13 of CNP's CSP with the following language found acceptable by NRC letter dated March 1, 2011, to NEI. This language meets the requirements of 10 CFR 73.54(h).

"I&M has established the necessary measures and governing procedures to ensure that sufficient records of items and activities affecting cyber security are developed, reviewed, approved, issued, used, and revised to reflect completed work.

The following are examples of records or supporting technical documentation that are retained as a record until the Commission terminates the license for which the records are developed. Superseded portions of these records are retained for three years unless otherwise specified by the Commission in accordance with the requirements of 10 CFR 73.54(h):

- Modification records for CDAs;
- Analyses, basis, conclusions, and determinations used to establish a component as a CDA;
- Cyber Security Plan;
- Written Policies and Procedures that implement and maintain the Cyber Security program, with records of changes;
- Corrective Action records related to Cyber Security non-conformance or adverse conditions;
- Documentation of periodic Cyber Security Program reviews and Program audits;
- Vulnerability notifications determined to adversely impact CDAs and the associated analyses, assessments and dispositions;
- Training records to document personnel qualifications and program implementation and maintenance; and
- Audit records are electronic or manual event records (logs) that facilitate the identification and analysis of cyber security attacks and are developed in accordance with Appendix D, Section 2, “*Audit and Accountability.*”
  - The scope of auditable events is developed in accordance with Appendix D, Section 2.2, “*Auditable Events.*” Events identified for auditing are recorded in accordance with Appendix D, Section 2.3, “*Content of Audible Events*” and Appendix D, Section 2.4, “*Audit Storage Capacity*” (for electronic audit records). The source of auditable events (electronic and non-electronic) include, but are not limited to:
    - Operating system logs
    - Service and application logs
    - Network device logs
    - Access logs
  - Audit records of auditable events are retained to document access history, as well as to discover the source of cyber attacks or other security-related incidents affecting CDAs or SSEP functions, or both. These records are reviewed and analyzed in accordance with [policies, procedures, programs] implementing Appendix D, Section 2.6, *Audit Review, Analysis and Reporting.* The review and analysis is conducted consistent with maintaining high assurance that digital computer and communication systems and networks are adequately protected against cyber attacks, up to and including the design basis threat as described in 10 CFR 73.1. Superseded records (or portions thereof) are then retained for three years, after the record has been reviewed and analyzed.”

## **NRC RAI Question 2**

*The regulation at 10 CFR 73.54, “Protection of digital computer and communication systems and networks,” requires licensees to submit a CSP that satisfies the requirements of this section*

for commission review and approval. Furthermore, each submittal must include a proposed implementation schedule and the implementation of the licensee's cyber security program must be consistent with the approved schedule. Paragraph 73.54(a) of 10 CFR requires licensees 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.

The completion of several key intermediate milestones (Items (a) through (g) below) would demonstrate progress toward meeting the requirements of 10 CFR 73.54. The Nuclear Regulatory Commission (NRC) staff's expectation is that the key intermediate milestones will be completed in a timely manner, but no later than December 31, 2012. The key CSP implementation milestones are as follows:

- (a) Establish, train and qualify Cyber Security Assessment Team, as described in Section 3.1.2, "Cyber Security Assessment Team," of the CSP.
- (b) Identify Critical Systems and CDAs, as described in Section 3.1.3, "Identification of Critical Digital Assets," of the CSP.
- (c) Implement cyber security defense-in-depth architecture by installation of [deterministic one-way] devices, as described in Section 4.3, "Defense-In-Depth Protective Strategies" of the CSP.
- (d) Implement the management, operational and technical cyber security controls that address attacks promulgated by use of portable media, portable devices, and portable equipment as described in Appendix D Section 1.19 "Access control for Portable and Mobile Devices," of nuclear Energy Institute (NEI) 08-09, Revision 6.
- (e) Implement observation and identification of obvious cyber related tampering to existing insider mitigation rounds as described in Appendix E Section 4.3, "Personnel Performing Maintenance and Testing Activities," and Appendix E Section 10.3, "Baseline configuration" of NEI 08-09, revision 6.
- (f) Identify, document, and implement cyber security controls to physical security target set CDAs in accordance with Section 3.1.6, "Mitigation of Vulnerabilities and Application of Cyber Security Controls," of the CSP.
- (g) Ongoing monitoring and assessment activities will commence for those target set CDAs whose security controls have been implemented, as described in Section 4.4, "Ongoing Monitoring and Assessment," of the CSP.
- (h) Full implementation of the CSP for all safety, security, and emergency preparedness functions.

Provide a revised CSP implementation schedule that identified the appropriate milestones, completion dates, supporting rationale, and level of detail to allow the NRC to evaluate the licensee's proposed schedule and associated milestone dates which include the final completion date. It is the NRC's intention to develop a license condition incorporating your revised CSP implementation schedule containing the key milestone dates.

## **I&M Response**

### **Cyber Security Plan Implementation Schedule**

Full implementation of the cyber security program involves many supporting tasks. Major activities include: program and procedure development; performing of individual critical digital

asset (CDA) assessments; and identification, scheduling, and implementing individual asset security control design remediation actions through the site configuration management program. These design modifications may be performed on-line or could require a refueling outage for installation.

The extensive workload associated with full implementation of the Cyber Security Plan (CSP) requires prioritization to assure those activities that provide higher degrees of protection against radiological sabotage are performed first. Therefore the CSP implementation schedule will be implemented with two major milestone dates. The first milestone date of no later than December 31, 2012, includes the activities that provide higher degrees of immediate protection. The second milestone date, December 31, 2014, includes the completion of all remaining actions that result in the full implementation of the cyber security plan for all applicable Safety, Security, and Emergency Preparedness (SSEP) functions. This date also bounds the completion of all individual asset security control design remediation actions.

Cyber security controls are not applied if the control adversely impacts safety and important to safety, security or emergency preparedness functions.

#	Implementation Milestone	Completion Date	Basis
1	Establish Cyber Security Assessment Team (CSAT) as described in Section 3.1.2 "Cyber Security Assessment Team" of the Cyber Security Plan (CSP).	I&M has completed this Milestone	The CSAT, collectively, will need to have digital plant systems knowledge as well as nuclear power plant operations, engineering and nuclear safety experience and technical expertise. The personnel selected for this team may require additional training in these areas help to ensure adequate capabilities to perform cyber security assessments as well as others duties.
2	Identify Critical Systems (CSs) and Critical Digital Assets (CDAs) as described in Section 3.1.3 "Identification of Critical Digital Assets" of the CSP.	I&M has completed this milestone	The scope of 10 CFR 73.54 includes digital computer and communication systems and networks associated with: safety-related and important-to safety functions; security functions; emergency preparedness functions, including offsite communications; and support systems and equipment which, if compromised, would adversely impact safety, security, or emergency preparedness functions. The scope of 10 CFR 73.54 includes structures, systems, and components (SSCs) that have a nexus to radiological health and safety and therefore can directly or

#	Implementation Milestone	Completion Date	Basis
			indirectly affect reactivity of a nuclear power plant and could result in an unplanned reactor shutdown or transient.
3	<p>Implement Installation of a deterministic isolation boundary device between lower level devices (level 0, 1,2) and the higher level devices (level 3,4) as described in Section 4.3, "Defense-In-Depth Protective Strategies" of the CSP.</p> <p>Lower security level devices (level 0, 1, 2 devices) that bypass the deterministic device and connect to level 3 or 4 will be modified to prevent the digital connectivity to the higher level or will be modified to meet cyber security requirements commensurate with the level 3 or 4 devices to which they connect.</p> <p>The design modifications that are not finished by the completion date will be documented in the site configuration management and/or change control program to assure completion of the design modification as soon as possible, but no later than the final implementation date.</p>	No later than December 31, 2012	The implementation of communication barriers protects the most critical SSEP functions from remote attacks on plant systems. Isolating the plant systems from the internet as well as from the corporate business systems is an important milestone in defending against external threats. While the deployment of the barriers is critical to protection from external cyber threats, it also prevents remote access to core monitoring and plant data systems for reactor engineers, plant operations, and other plant staff. This elimination of remote access to reactor core monitoring systems may require the development and execution of a detailed change management plan to ensure continued safe operation of the plants. Vendors may be required to develop software revisions to support the model. The modification will be developed, prioritized and scheduled.
4	The security control "Access Control For Portable And Mobile Devices" described in Appendix D 1.19 of NEI 08-09, Revision 6, will be implemented.	No later than December 31, 2012	Portable media devices are used to transfer electronic information (e.g., data, software, firmware, virus engine updates and configuration information) to and from plant process equipment. Careful use of this class of media is required to minimize the spread of malicious software to plant process

#	Implementation Milestone	Completion Date	Basis
			equipment. The effective implementation of this control may require the coordinated implementation of other complimentary controls to ensure adequate mitigation.
5	Implement observation and identification of obvious cyber related tampering to existing insider mitigation rounds by incorporating the appropriate elements in Appendix E Section 4.3 "Personnel Performing Maintenance And Testing Activities."	No later than December 31, 2012	Insider mitigation rounds by trained staff look for obvious signs of cyber related tampering and would provide mitigation of observable cyber related insider actions. Implementing steps to add signs of cyber security-related tampering to insider mitigation rounds will be performed by the completion date.
6	<p>Identify, document, and implement cyber security controls in accordance with the Cyber Security Plan Section 3.1.6 "Mitigation of Vulnerabilities and Application of Cyber Security Controls" for CDAs that could adversely impact the design function of physical security target set equipment.</p> <p>The implementation of controls that require a design modification that are not finished by the completion date will be documented in the site configuration management and/or change control program to assure completion of the design modification as soon as possible, but no later than the final implementation date.</p>	No later than December 31, 2012	The site physical protection program provides high assurance that these elements are protected from physical harm by an adversary. The cyber security program will enhance the defense-in-depth nature of the protection of CDAs associated with target sets. Implementing Cyber Security Plan security controls to target set CDAs provides a high degree of protection against a cyber related attacks that could lead to radiological sabotage. Security controls will be addressed in accordance with Cyber Security Plan Section 3.1.6 with the exception of those that require a design modification.
7	Ongoing monitoring and assessment activities commence, as described in Section 4.4, "Ongoing Monitoring and Assessment" of	No later than December 31, 2012	The ongoing monitoring and assessment activities as described in Section 4.4, "Ongoing Monitoring and Assessment" of the Cyber Security Plan will be implemented for the

#	Implementation Milestone	Completion Date	Basis
	the CSP, for those target set CDAs whose security controls have been implemented.		controls applied to target set CDAs. This action results in the commencement of the cyber security program for target set related CDAs.
8	Full implementation of the CNP Cyber Security Plan for all SSEP functions will be achieved.	December 31, 2014	By the completion date, the CNP Cyber Security Plan will be fully implemented for all SSEP functions in accordance with 10 CFR 73.54. This date also bounds the completion of all individual asset security control design remediation actions including those that require a refuel outage for implementation.

The above implementation schedule supersedes, in its entirety, the previous implementation schedule that was previously submitted by letter dated July 19, 2010, for NRC approval. This implementation schedule is identified as Regulatory Commitments in Enclosure 3 to this letter.

### NRC RAI Question 3

*Paragraph 73.54(a) of 10 CFR requires licensees 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 as described in 10 CFR 73.1. In addition, 10 CFR 73.54(a)(1) states that the licensee shall protect digital computer and communication systems and networks associated with:*

- (i) Safety-related and important-to-safety functions;*
- (ii) Security functions;*
- (iii) Emergency preparedness functions, including offsite communications; and*
- (iv) Support systems and equipment which, if compromised, would adversely impact safety, security, or emergency preparedness functions.*

*Subsequent to the issuance of the cyber security rule, the NRC stated that 10 CFR 73.54 should be interpreted to include structures, systems, and components (SSCs) in the balance of plant (BOP) that have a nexus to radiological health and safety (Agencywide Documents Access and Management System (ADAMS) Accession No. ML103490344, dated November 19, 2010). The SSCs in the BOP are those that could directly or indirectly affect reactivity of a nuclear power plant and could result in an unplanned reactor shutdown or transient and are therefore, within the scope of important-to-safety functions described in 10 CFR 73.54(a)(1). Furthermore, the NRC issued a letter to NEI dated January 5, 2011 (ADAMS Accession No. ML103550480) that provided licensees with additional guidance on one acceptable approach to comply with the commission's policy determination.*

*Explain how the scoping of systems provided by CNP's CSP meets the requirements of 10 CFR 73.54 and the additional guidance provided by the NRC.*

**I&M Response**

By letter dated January 5, 2011, the NRC provided NEI verbiage for licensees to incorporate into their CSP in order to meet the requirements of 10 CFR 73.54. This verbiage has been reviewed by CNP and the following will be added into the CNP CSP Section 2.1.

"Within the scope of NRC's cyber security rule at 10 CFR 73.54, systems or equipment that perform important to safety functions include SSCs in the balance of plant that could directly or indirectly affect reactivity at a nuclear power plant and could result in an unplanned reactor shutdown or transient. Additionally, these SSCs are under the licensee's control and include electrical distribution equipment out to the first inter-tie with the offsite distribution system."

Enclosure 3 to AEP-NRC-2011-18

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. The following commitments supersede, in their entirety, the commitments made by letter dated July 19, 2010, which provided the proposed implementation schedule as required by 10 CFR 73.54.

Commitment	Completion Date
<p>Implement Installation of a deterministic isolation boundary device between lower level devices (level 0, 1,2) and the higher level devices (level 3,4) as described in Section 4.3, "Defense-In-Depth Protective Strategies" of the CSP.</p> <p>Lower security level devices (level 0, 1, 2 devices) that bypass the deterministic device and connect to level 3 or 4 will be modified to prevent the digital connectivity to the higher level or will be modified to meet cyber security requirements commensurate with the level 3 or 4 devices to which they connect.</p> <p>The design modifications that are not finished by the completion date will be documented in the site configuration management and/or change control program to assure completion of the design modification as soon as possible, but no later than the final implementation date. (This item is being tracked by I&amp;M as a separate commitment listed below).</p>	December 31, 2012
<p>The design modifications that are not finished by the completion date will be documented in the site configuration management and/or change control program to assure completion of the design modification as soon as possible, but no later than the final implementation date.</p>	December 31, 2014
<p>The security control "Access Control For Portable And Mobile Devices" described in Appendix D 1.19 of NEI 08-09, Revision 6, will be implemented.</p>	December 31, 2012
<p>Implement observation and identification of obvious cyber related tampering to existing insider mitigation rounds by incorporating the appropriate elements in Appendix E Section 4.3 "Personnel Performing Maintenance And Testing Activities."</p>	December 31, 2012
<p>Identify, document, and implement cyber security controls in accordance with the Cyber Security Plan Section 3.1.6 "Mitigation of Vulnerabilities and Application of Cyber Security Controls" for CDAs</p>	December 31, 2012

Commitment	Completion Date
<p>that could adversely impact the design function of physical security target set equipment.</p> <p>The implementation of controls that require a design modification that are not finished by the completion date will be documented in the site configuration management and/or change control program to assure completion of the design modification as soon as possible, but no later than the final implementation date. (This item is being tracked by I&amp;M as a separate commitment listed below).</p>	
<p>The implementation of controls that require a design modification that are not finished by the completion date will be documented in the site configuration management and/or change control program to assure completion of the design modification as soon as possible, but no later than the final implementation date.</p>	December 31, 2014
<p>Ongoing monitoring and assessment activities commence, as described in Section 4.4, "Ongoing Monitoring and Assessment" of the CSP, for those target set CDAs whose security controls have been implemented.</p>	December 31, 2012
<p>Full implementation of the CNP Cyber Security Plan for all SSEP functions will be achieved.</p>	December 31, 2014