

From: Wengert, Thomas
Sent: Friday, January 07, 2011 1:16 PM
To: Vincent, Dale M.
Cc: Tam, Peter
Subject: XCEL (Monticello and Prairie Island) Cyber Security Plan LAR - Draft RAI #1 (TAC Nos. ME4272, ME4294, and ME4295)
Attachments: XCEL Draft RAI#1 for CSP LAR.pdf

Dale,

See attached Draft RAI #1 for the subject LAR. Please review and let me know if you would like me to arrange a telecon with the NRC staff to clarify the request. Also, let's discuss the response time for these RAIs.

Regards,

Tom Wengert
USNRC
Project Manager – Prairie Island
NRR/DORL/LPLIII-1
(301) 415-4037

REQUEST FOR ADDITIONAL INFORMATION (RAI)
REGARDING APPROVAL OF CYBER SECURITY PLAN
NORTHERN STATES POWER COMPANY – MINNESOTA
MONTICELLO NUCLEAR GENERATING PLANT, UNIT 1
PRAIRIE ISLAND NUCLEAR GENERATING PLANT, UNITS 1 AND 2
DOCKET NOS. 50-263, 50-282, AND 50-306

Cyber Security Plan (CSP) Section 4: Establishing, Implementing, and Maintaining the Cyber Security Program

RAI 1: Clarifying the Site Defensive Model

Title 10 of the *Code of Federal Regulations* (10 CFR) Section 73.54 (c)(2) calls for the licensee to “apply and maintain defense-in-depth protective strategies...” and 10 CFR 73.54(d)(2) calls for the licensee to evaluate and manage cyber risks.

Nuclear Energy Institute (NEI) 08-09 Rev. 6, page A-12, section 4.3, provides two examples of an effective defensive model to meet the requirements of 10 CFR 73.54. Example 1 states (in part): Information flows between Levels 3 and 4 are restricted through the use of a firewall and a network-based intrusion detection system. Example 2 states (in part): Information flows between security critical digital assets (CDAs) in one level and security CDAs in another level are restricted through the use of a firewall and a network-based intrusion detection system.

The Monticello and Prairie Island CSP (as found on page 12, section 4.3, third paragraph) states (in part): The boundary between Level 3 and Level 2 is implemented by one or more **devices or methods** that isolate CDAs in or above Level 3. Information flows between Levels 3 and 4 are restricted through the use of defense-in-depth techniques that utilize technologies **such as** firewalls and network-based intrusion detection systems and strategic local area network architecture designs.

There are two parts to the RAI, but both relate to the defensive architecture:

1. What are the “**devices or methods**” (these words are not used in the NEI 08-09 template) referred to in the Monticello and Prairie Island CSP? Provide an explanation of how this is equivalent to unidirectional communication devices (e.g., data diodes) or air gaps.
2. The Monticello and Prairie Island CSP uses the term “**such as**”, which means these are just examples and the application of only one approach (e.g., a firewall alone) may suffice. Clarify how this approach is equivalent to an approach that incorporates both a firewall and a network intrusion detection system (i.e., two independent protection methods).

Enclosure

RAI 2: Timeframe for Verifying Security Controls

Section 73.54(g) of 10 CFR states: "The licensee shall review the cyber security program as a component of the physical security program in accordance with the requirements of § 73.55(m), including the periodicity requirements." And, 10 CFR 73.55(m) states that the Security Program be reviewed: "(1) As a minimum the licensee shall review each element of the physical protection program at least every 24 months."

Monticello and Prairie Island CSP states on page 14, section 4.4.3, last paragraph: Ongoing assessments are performed to verify that the cyber security controls implemented for CDAs remain in place throughout the life cycle. The assessment process verifies the status of these cyber security controls **at least every 36 months** or in accordance with the specific requirements for utilized cyber security controls as described in Appendices D and E of NEI 08-09, Revision 6, whichever is more frequent.

Clarify how a periodicity of 36 months for the assessment of cyber security controls meets the requirements of 10 CFR 73.55(m) for 24 months.

DRAFT