

ENCLOSURES 1 and 2 CONTAIN SECURITY-RELATED INFORMATION  
WITHHOLD UNDER 10 CFR 2.390



414 Nicollet Mall – MP4  
Minneapolis, MN 55401

April 1, 2011

L-XE-11-004  
10 CFR 50.90

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

Prairie Island Nuclear Generating Plant,  
Units 1 and 2  
Dockets 50-282 and 50-306  
License Nos. DPR-42 and DPR-60

Monticello Nuclear Generating Plant  
Docket 50-263  
Renewed License No. DPR-22

Supplement to License Amendment Request (LAR) for Approval of the Northern States Power Company - Minnesota Cyber Security Plan (TAC Nos. ME4294, ME4295, and ME4272)

By letter dated July 20, 2010, (Agencywide Documents Access and Management System (ADAMS) Accession No. ML102020164), Northern States Power Company, a Minnesota corporation, doing business as Xcel Energy (hereafter "NSPM"), submitted an LAR for the Prairie Island Nuclear Generating Plant (PINGP), Units 1 and 2, and the Monticello Nuclear Generating Plant (MNGP) requesting Nuclear Regulatory Commission (NRC) approval of the NSPM Cyber Security Plan (CSP), proposed implementation schedule, and addition of a sentence to the existing PINGP and MNGP Facility Operating Licenses (FOL) Physical Protection license conditions to require NSPM to fully implement and maintain in effect all provisions of the Commission approved CSP. NSPM supplemented the LAR requesting approval of the NSPM CSP by letters dated November 30, 2010 (ADAMS Accession No. ML103350163), and February 21, 2011 (ADAMS Accession No. ML110540144).

By letter dated March 4, 2011 (ADAMS Accession Number ML 110600980), NRC Staff requested additional information to support their review of the July 20, 2010 submittal and its supplements. Enclosure 1 to this letter provides the responses to the NRC Staff requests for additional information (RAIs). Enclosure 2 provides the CSP revised to incorporate the changes discussed in the RAI responses. NSPM submits this supplement in accordance with the provisions of 10 CFR 50.90.

Enclosure 4 to the submittal dated July 20, 2010 (ADAMS Accession No. ML102020164), included six commitments to implementation milestone dates and the date for full CSP implementation. By this letter NSPM withdraws the six commitments to implementation milestone dates provided in the July 20, 2010 letter. NRC RAI 2 states, "It is the NRC's intention to develop a license condition incorporating your

revised CSP implementation schedule containing the key milestone dates.” NSPM believes milestone activity completion dates should be commitments in lieu of an NRC license condition and this letter makes seven new commitments stated below based on the response to RAI 2 in Enclosure 1.

NSPM understands that the NRC withheld the NSPM CSP submitted with the July 20, 2010 (ADAMS Accession No. ML102020164), from public disclosure as security sensitive information. Accordingly, Enclosures 1 and 2 to this letter have been marked as security related and NSPM requests that they be withheld from public disclosure in accordance with 10CFR 2.390.

The supplemental information provided in this letter does not impact the conclusions of the Determination of No Significant Hazards Consideration or Environmental Assessment presented in the July 20, 2010 submittal as supplemented November 30, 2010 and February 21, 2011.

In accordance with 10 CFR 50.91, NSPM is notifying the State of Minnesota of this LAR supplement by transmitting a copy of this letter to the designated State Official.

If you have questions regarding this submittal, please contact Mr. Dale Vincent, P.E., at 651-388-1121.

#### Summary of Commitments

This letter withdraws the six implementation milestone dates included in Enclosure 4 to the July 20, 2010 (ADAMS Accession No. ML102020164), submittal and makes the following new commitments:

1. By December 31, 2012, establish Cyber Security Assessment Team (CSAT) as described in Section 3.1.2 “Cyber Security Assessment Team” of the Cyber Security Plan (CSP).
2. By December 31, 2012, identify Critical Systems (CSs) and Critical Digital Assets (CDAs) as described in Section 3.1.3 “Identification of Critical Digital Assets” of the CSP.
3. By December 31, 2012, implement installation of a deterministic one way device or a combination of technologies consisting of firewall devices and intrusion detection/ intrusion prevention systems 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.

By December 31, 2012, 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.

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.

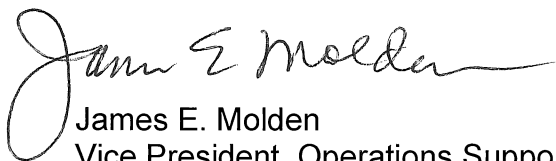
4. By December 31, 2012, the security control "Access Control For Portable And Mobile Devices" described in Appendix D 1.19 of NEI 08-09, Revision 6, will be implemented.
5. By December 31, 2012, implement observation and identification of obvious cyber related tampering to existing insider mitigation rounds by incorporating the appropriate elements in Appendix E Section 4.3 "Personnel Performing Maintenance And Testing Activities."
6. By December 31, 2012, identify, document, and implement NEI 08-09, Rev 6, Appendix D, technical 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.

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.

7. By December 31, 2012, 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.

I declare under penalty of perjury that the foregoing is true and correct.

Executed on April 1, 2011.



James E. Molden  
Vice President, Operations Support  
Northern States Power Company - Minnesota

Enclosures (2)

cc: Administrator, Region III, USNRC  
Project Manager, PINGP, USNRC

Document Control Desk

Page 4

Resident Inspector, PINGP, USNRC  
Project Manager, MNGP, USNRC  
Resident Inspector, MNGP, USNRC  
State of Minnesota (letter only)