



Matthew W. Sunseri
Vice President Operations and Plant Manager

November 23, 2009

WO 09-0044

U. S. Nuclear Regulatory Commission
ATTN: Document Control Desk
Washington, D. C. 20555

Reference: NEI 08-09, "Cyber Security Plan for Nuclear Power Reactors,"
Revision 3

Subject: Docket No. 50-482: Revision to Renewed Facility Operating
License and Request for Approval of the Cyber Security Plan

Gentlemen,

Pursuant to 10 CFR 50.90, Wolf Creek Nuclear Operating Corporation (WCNOC) is submitting a request for an amendment to Renewed Facility Operating License No. NPF-42 for the Wolf Creek Generating Station (WCGS) and requesting Commission review and approval of a cyber security plan in accordance with 10 CFR 73.54. WCNOC is proposing to revise Section 2.E. of the Renewed Facility Operating License to incorporate the provisions for implementing and maintaining in effect the provisions of the approved cyber security plan.

Attachment I provides an evaluation of the proposed change. Attachment II provides the existing Renewed Facility Operating License marked up to show the proposed change. Attachment III provides the Renewed Facility Operating License changes in final typed format. Attachment IV provides a List of Regulatory Commitments made in this submittal.

Enclosure I provides a copy of the Cyber Security Plan for Wolf Creek Nuclear Operating Corporation, Wolf Creek Generating Station, which is a standalone document that will be incorporated by reference into the Wolf Creek Security Plan, Training and Qualification Plan, and Safeguards Contingency Plan upon approval. The cyber security plan is consistent with guidance in the Reference. Enclosure II provides a copy of the Cyber Security Plan Implementation Schedule. Enclosure III provides a Deviation Table which includes a description of changes to the un-bracketed text of Nuclear Energy Institute (NEI) 08-09, Revision 3. WCNOC requests that the enclosures, which contain security-related information, be withheld from public disclosure in accordance with 10 CFR 2.390.

NOTE: Enclosures I, II, and III to this letter contain "Security-Related Information" and should be withheld from public disclosure in accordance with 10 CFR 2.390. When separated from these enclosures this letter is "Decontrolled."

SOO1
NRK

WO 09-0044

Page 2 of 3

WCNOC requests approval of the proposed License Amendment by November 23, 2010, to be implemented in conjunction with the issuance of the approved Cyber Security Plan for Wolf Creek Nuclear Operating Corporation, Wolf Creek Generating Station, within 120 days of the issuance of the license amendment.

It has been determined that this amendment application does not involve a significant hazard consideration as determined per 10 CFR 50.92. This amendment application was reviewed by the Plant Safety Review Committee. In accordance with 10 CFR 50.91, a copy of this amendment application, with attachments, is being provided to the designated Kansas State official.

If you have any questions concerning this matter, please contact me at (620) 364-4008, or Mr. Richard D. Flannigan, Manager Regulatory Affairs at (620) 364-4117.

Sincerely,



Matthew W. Sunseri

MWS/rit

- Attachment:
- I Evaluation of Proposed Change
 - II Proposed Renewed Facility Operating License Changes (Mark-up)
 - III Retyped Renewed Facility Operating License Changes
 - IV List of Regulatory Commitments
- Enclosure:
- I Cyber Security Plan for Wolf Creek Nuclear Operating Corporation, Wolf Creek Generating Station
 - II Cyber Security Plan Implementation Schedule
 - III Deviation Table (Description of Changes to Un-Bracketed Text of NEI 08-09, Revision 3)

cc: E. E. Collins (NRC), w/a, w/e
T. A. Conley, (KDHE), w/a
G. B. Miller (NRC), w/a, w/e
B. K. Singal (NRC), w/a, w/e
Senior Resident Inspector (NRC), w/a, w/e

NOTE: Enclosures I, II, and III to this letter contain "Security-Related Information" and should be withheld from public disclosure in accordance with 10 CFR 2.390. When separated from these enclosures this letter is "Decontrolled."

WO 09-0044
Page 3 of 3

STATE OF KANSAS)
) SS
COUNTY OF COFFEY)

Matthew W. Sunseri, of lawful age, being first duly sworn upon oath says that he is Vice President Operations and Plant Manager of Wolf Creek Nuclear Operating Corporation; that he has read the foregoing document and knows the contents thereof; that he has executed the same for and on behalf of said Corporation with full power and authority to do so; and that the facts therein stated are true and correct to the best of his knowledge, information and belief.

By Matthew W. Sunseri
Matthew W. Sunseri
Vice President Operations and Plant Manager

SUBSCRIBED and sworn to before me this 23rd day of November, 2009.

Cindy Novinger
Notary Public



Expiration Date 7/8/2010

NOTE: Enclosures I, II, and III to this letter contain "Security-Related Information" and should be withheld from public disclosure in accordance with 10 CFR 2.390. When separated from these enclosures this letter is "Decontrolled."

EVALUATION OF PROPOSED CHANGE

Subject: Revision to Renewed Facility Operating License and Request for Approval of the Cyber Security Plan

1. SUMMARY DESCRIPTION
2. DETAILED DESCRIPTION
3. TECHNICAL EVALUATION
4. REGULATORY EVALUATION
 - 4.1 Applicable Regulatory Requirements/Criteria
 - 4.2 Significant Hazards Consideration
 - 4.3 Conclusions
5. ENVIRONMENTAL CONSIDERATION
6. REFERENCES

1. SUMMARY DESCRIPTION

Pursuant to 10 CFR 50.90, Wolf Creek Nuclear Operating Corporation (WCNOC) is submitting a request for an amendment to Renewed Facility Operating License No. NPF-42 for the Wolf Creek Generating Station (WCGS) and requesting Commission review and approval of a cyber security plan in accordance with 10 CFR 73.54. WCNOC is proposing to revise Section 2.E. of the Renewed Facility Operating License to incorporate the provisions for implementing and maintaining in effect the provisions of the approved cyber security plan.

2. DETAILED DESCRIPTION

The proposed license amendment request (LAR) includes three parts: the proposed cyber security plan, proposed changes to Section 2.E. of the Renewed Facility Operating License, and a Cyber Security Plan Implementation Schedule.

A new paragraph is proposed to be added to paragraph 2.E. of the Renewed Facility Operating License as follows:

The licensee shall fully implement and maintain in effect all provisions of the Commission-approved Cyber Security Plan, including amendments made pursuant to provision of the Miscellaneous Amendments and Search Requirements revisions to 10 CFR 73.55 (51 FR 27817 and 27822) and to the authority of 10 CFR 50.90 and 10 CFR 50.54(p). The Cyber Security Plan entitled: "Cyber Security Plan for Wolf Creek Nuclear Operating Corporation, Wolf Creek Generating Station," which contains Security-Related Information is withheld from public disclosure in accordance with 10 CFR 2.390, was submitted on November 23, 2009.

The regulations in 10 CFR 73.54, "Protection of digital computer and communication systems and networks," establish the requirements for a cyber security program. This regulation specifically requires each licensee currently licensed to operate a nuclear power plant under Part 50 of this chapter 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 cyber security program must be consistent with the approved schedule. Enclosure I provides the Cyber Security Plan for Wolf Creek Nuclear Operating Corporation, Wolf Creek Generating Station (Cyber Security Plan). Enclosure II provides the Cyber Security Plan Implementation Schedule.

3. TECHNICAL EVALUATION

Federal Register notice 74 FR 13926 (Reference 1) issued the final rule that amended 10 CFR Part 73. Cyber security requirements are codified as new 10 CFR 73.54 and 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 § 73.1(a)(1)(v). These requirements are substantial improvements upon the requirements imposed by EA-02-026 (Reference 2).

Nuclear Energy Institute (NEI) 08-09, Revision 3, September 2009, "Cyber Security Plan for Nuclear Power Plants," (Reference 3) has been issued for use by licensees in development of their own cyber security plans. NEI 08-09 describes a defensive strategy that consists of a defensive architecture and set of security controls that are based on the NIST SP 800-82, Final Public Draft, dated September 29, 2008, "Guide to Industrial Control System Security," and NIST SP 800-53, Revision 2, "Recommended Security Controls for Federal Information Systems" standards. The security controls contained in NEI 08-09 Appendices D and E are tailored for use in nuclear facilities and are based on NIST SP 800-82 and NIST SP 800-53.

This amendment request includes a proposed Cyber Security Plan (Enclosure I) that is consistent with the template provided in NEI 08-09, Revision 3. In addition, the amendment request includes proposed changes to paragraph 2.E. of the existing Renewed Facility Operating License (Attachment II). A proposed Cyber Security Plan Implementation Schedule as required by 10 CFR 73.54 is provided in Enclosure II. Enclosure III provides a Deviation Table that provides a description of the changes to the un-bracketed text of NEI 08-09, Revision 3, and a justification for those changes.

4. REGULATORY EVALUATION

4.1 Applicable Regulatory Requirements/Criteria

10 CFR 73.54 requires licensees currently licensed to operate a nuclear power plant under 10 CFR Part 50 to submit a cyber security plan as specified in 50.4 and 50.90. 10 CFR 50.73(a) requires each licensee subject to the requirements of this section shall 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.

4.2 No Significant Hazards Consideration

WCNOC has evaluated whether or not 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. Do the proposed changes involve a significant increase in the probability 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 Cyber Security Plan for Wolf Creek Nuclear Operating Corporation, Wolf Creek Generating Station (Cyber Security Plan) for NRC review and approval. The Cyber Security Plan is consistent with the template provided in NEI 08-09, Revision 3, and provides a description of how the requirements of the Rule will be implemented at WCGS. The Cyber Security Plan establishes the licensing basis for the WCNOC Cyber Security Program. The Cyber Security Plan also 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:

- 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.

Part one of the proposed change is designed to achieve high assurance that the systems are protected from cyber attacks. The Cyber Security Plan itself does not require any plant modifications. However, the Cyber Security Plan does describe how plant modifications which involve digital computer systems are reviewed to provide high assurance of adequate protection against cyber attacks, up to and including the design basis threat as defined in the Rule. The proposed change 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 first part of the proposed change is designed to achieve high assurance that the systems within the scope of the Rule are protected from cyber attacks and has no impact on the probability or consequences of an accident previously evaluated.

The second part adds a paragraph to Section 2.E. of the existing Renewed Facility Operating License. The third part of the proposed change is a Cyber Security Plan Implementation Schedule. Both of these changes are administrative and have no impact on the probability or consequences of an accident previously evaluated.

Therefore, the proposed changes do not involve a significant increase in the probability or consequences of an accident previously evaluated.

2. Do the proposed changes create the possibility of a new or different kind of accident from any 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 Cyber Security Plan for NRC review and approval. The Cyber Security Plan is consistent with the template provided by NEI 08-09, Revision 3 and provides a description of how the requirements of the Rule will be implemented at WCGS. The Cyber Security Plan establishes the licensing basis for the WCNOG Cyber Security Program. The Cyber Security Plan also 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:

- 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.

Part one of the proposed change is designed to achieve high assurance that the systems within the scope of the Rule are protected from cyber attacks. The Cyber Security Plan itself does not require any plant modifications. However, the Cyber Security Plan does describe how plant modifications involving digital computer systems are reviewed to provide high assurance of

adequate protection against cyber attacks, up to and including the design basis threat defined in the Rule. The proposed change 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 first part of the proposed change is designed to achieve 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 adds a paragraph to Section 2.E. of the existing Renewed Facility Operating License. The third part of the proposed change is a Cyber Security Plan Implementation Schedule. 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. Do the proposed changes involve a significant reduction in a margin of safety?

Response: No

The proposed change is required by § 73.54 and includes three parts. The first part is the submittal of the Cyber Security Plan for NRC review and approval. The Cyber Security Plan is consistent with the template provided by NEI 08-09, Revision 3, and provides a description of how the requirements of the Rule will be implemented at WCGS. The Cyber Security Plan establishes the licensing basis for the WCNOG Cyber Security Program. The Cyber Security Plan also 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:

- 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.

Part one of the proposed change is designed to achieve 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 adds a paragraph to Section 2.E. of the existing Renewed Facility Operating License. The third part of the proposed change is a Cyber Security Plan Implementation Schedule. 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 reduction in a margin of safety.

Based on the above evaluations, WCNOC concludes that the proposed amendment presents no significant hazards under the standards set forth in 10 CFR 50.92(c) and, accordingly, a finding of "no significant hazards consideration" is justified.

4.3 Conclusions

The proposed licensing action requests an amendment to Renewed Facility Operating License No. NPF-42 for the WCGS and requests Commission review and approval of a cyber security plan in accordance with 10 CFR 73.54. 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.

5. ENVIRONMENTAL CONSIDERATION

WCNOC has evaluated the proposed change and has determined that the change does not involve (i) a significant hazards consideration, (ii) a significant change in the types or significant increase in the amount of effluent that may be released offsite, or (iii) a significant increase in the individual or cumulative occupational radiation exposure. Accordingly, the proposed changes meets the eligibility criterion for categorical exclusion set forth in 10 CFR 51.22(c)(9). Therefore, pursuant to 10 CFR 51.22(b), an environmental assessment of the proposed change is not required.


6. 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.
3. NEI 08-09, Revision 3, September 2009, "Cyber Security Plan for Nuclear Power Reactors

PROPOSED RENEWED FACILITY OPERATING LICENSE CHANGES (MARK-UP)

(16) Additional conditions

The Additional Conditions contained in Appendix D, as revised through Amendment No. 163, are hereby incorporated into this license. Wolf Creek Nuclear Operating Corporation shall operate the facility in Accordance with the Additional Conditions.

- D. Exemptions from certain requirements of Appendix J to 10 CFR Part 50, and from a portion of the requirements of General Design Criterion 4 of Appendix A to 10 CFR Part 50, are described in the Safety Evaluation Report. These exemptions are authorized by law and will not endanger life or property or the common defense and security and are otherwise in the public interest. Therefore, these exemptions are hereby granted pursuant to 10 CFR 50.12. With the granting of these exemptions the facility will operate, to the extent authorized herein, in conformity with the application, as amended, the provisions of the Act, and the rules and regulations of the Commission.
- E. The licensee shall fully implement and maintain in effect all provisions of the Commission-approved physical security, training and qualification, and safeguards contingency plans including amendments made pursuant to provisions of the Miscellaneous Amendments and Search Requirements revisions to 10 CFR 73.55 (51 FR 27817 and 27822) and to the authority of 10 CFR 50.90 and 10 CFR 50.54(p). The set of combined plans, which contains Safeguards Information protected under 10 CFR 73.21, is entitled: "Wolf Creek Security Plan, Training and Qualification Plan, and Safeguard Contingency Plan," and was submitted on May 17, 2006.
-  F. Deleted per Amendment No. 141.
- G. The licensees shall have and maintain financial protection of such type and in such amounts as the Commission shall require in accordance with Section 170 of the Atomic Energy Act of 1954, as amended, to cover public liability claims.
- H. The Updated Safety Analysis Report (USAR) supplement, as revised, submitted pursuant to 10 CFR 54.21(d), shall be included in the next scheduled update to the USAR required by 10 CFR 50.71(e)(4), as appropriate, following the issuance of this renewed operating license. Until that update is complete, WCNOC may make changes to the programs and activities described in the supplement without prior Commission approval, provided that WCNOC evaluates such changes pursuant to the criteria set forth in 10 CFR 50.59 and otherwise complies with the requirements in that section.
- I. The USAR supplement, as revised, describes certain future activities to be completed prior to the period of extended operation. WCNOC shall complete these activities by the dates specified in the applicable USAR section, but in no event, any later than March 11, 2025. WCNOC shall notify the Nuclear Regulatory Commission (NRC) in writing when implementation of these activities is complete and can be verified by NRC inspection.

INSERT A

The licensee shall fully implement and maintain in effect all provisions of the Commission-approved Cyber Security Plan, including amendments made pursuant to provision of the Miscellaneous Amendments and Search Requirements revisions to 10 CFR 73.55 (51 FR 27817 and 27822) and to the authority of 10 CFR 50.90 and 10 CFR 50.54(p). The Cyber Security Plan entitled: "Cyber Security Plan for Wolf Creek Nuclear Operating Corporation, Wolf Creek Generating Station," which contains Security-Related Information is withheld from public disclosure in accordance with 10 CFR 2.390, was submitted on November 23, 2009.

RETPED RENEWED FACILITY OPERATING LICENSE CHANGES

(16) Additional Conditions

The Additional Conditions contained in Appendix D, as revised through Amendment No. 163, are hereby incorporated into this license. Wolf Creek Nuclear Operating Corporation shall operate the facility in Accordance with the Additional Conditions.

- D. Exemptions from certain requirements of Appendix J to 10 CFR Part 50, and from a portion of the requirements of General Design Criterion 4 of Appendix A to 10 CFR Part 50, are described in the Safety Evaluation Report. These exemptions are authorized by law and will not endanger life or property or the common defense and security and are otherwise in the public interest. Therefore, these exemptions are hereby granted pursuant to 10 CFR 50.12. With the granting of these exemptions the facility will operate, to the extent authorized herein, in conformity with the application, as amended, the provisions of the Act, and the rules and regulations of the Commission.
- E. The licensee shall fully implement and maintain in effect all provisions of the Commission-approved physical security, training and qualification, and safeguards contingency plans including amendments made pursuant to provisions of the Miscellaneous Amendments and Search Requirements revisions to 10 CFR 73.55 (51 FR 27817 and 27822) and to the authority of 10 CFR 50.90 and 10 CFR 50.54(p). The set of combined plans, which contains Safeguards Information protected under 10 CFR 73.21, is entitled: "Wolf Creek Security Plan, Training and Qualification Plan, and Safeguard Contingency Plan," and was submitted on May 17, 2006.
- The licensee shall fully implement and maintain in effect all provisions of the Commission-approved Cyber Security Plan, including amendments made pursuant to provision of the Miscellaneous Amendments and Search Requirements revisions to 10 CFR 73.55 (51 FR 27817 and 27822) and to the authority of 10 CFR 50.90 and 10 CFR 50.54(p). The Cyber Security Plan entitled: "Cyber Security Plan for Wolf Creek Nuclear Operating Corporation, Wolf Creek Generating Station," which contains Security-Related Information is withheld from public disclosure in accordance with 10 CFR 2.390, was submitted on November 23, 2009.
- F. Deleted per Amendment No. 141.
- G. The licensees shall have and maintain financial protection of such type and in such amounts as the Commission shall require in accordance with Section 170 of the Atomic Energy Act of 1954, as amended, to cover public liability claims.
- H. The Updated Safety Analysis Report (USAR) supplement, as revised, submitted pursuant to 10 CFR 54.21(d), shall be included in the next scheduled update to the USAR required by 10 CFR 50.71(e)(4), as appropriate, following the issuance of this renewed operating license. Until that update is complete, WCNOC may make changes to the programs and activities described in the supplement without prior Commission approval, provided that WCNOC evaluates such changes pursuant to the criteria set forth in 10 CFR 50.59 and otherwise complies with the requirements in that section.
- I. The USAR supplement, as revised, describes certain future activities to be completed prior to the period of extended operation. WCNOC shall complete these activities by the dates specified in the applicable USAR section, but in no event, any later than March 11, 2025. WCNOC shall notify the Nuclear Regulatory Commission (NRC) in writing when implementation of these activities is complete and can be verified by NRC inspection.

LIST OF REGULATORY COMMITMENTS

The following table identifies those actions committed to by WCNOG in this document. Any other statements in this submittal are provided for information purposes and are not considered to be regulatory commitments. Please direct questions regarding these commitments to Mr. Richard Flannigan at (620) 364-4117.

Regulatory Commitments	Due Date / Event
The analysis of digital computer systems and networks in accordance with Section 3 of the Cyber Security Plan will be performed and results documented as required.	36 months after NRC approval of Cyber Security Plan
For cyber security controls that have been identified for implementation by the process described in Section 3, an implementation plan will be prepared and available for on-site inspection.	48 months after NRC approval of Cyber Security Plan (All CDA remediations budgeted, planned, scheduled and approved)
The elements to establish, implement, and maintain the Cyber Security Program as described in Chapter 4 of the Cyber Security Plan will be implemented. Schedule will be available onsite for inspection.	60 months after NRC approval of Cyber Security Plan (some remediations may be open beyond this period pending completion of scheduled modifications)