

# WOLF CREEK NUCLEAR OPERATING CORPORATION

Matthew W. Sunseri  
Vice President Operations and Plant Manager

December 21, 2009

WO 09-0053

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

Reference: Letter WO 09-0044 dated November 23, 2009, from M. W. Sunseri, WCNOG, to USNRC

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

Gentlemen,

The Reference submitted a request by Wolf Creek Nuclear Operating Corporation (WCNOG) to amend the Renewed Facility Operating License No. NPF-42 for the Wolf Creek Generating Station (WCGS). The proposed amendment requested Nuclear Regulatory Commission (NRC) approval of the "Cyber Security Plan for Wolf Creek Nuclear Operating Corporation, Wolf Creek Generating Station," provided a proposed Cyber Security Plan Implementation Schedule, and proposed a revision to Section 2.E of the 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 to the Reference provided WCNOG's evaluation of the proposed change and included a determination that the proposed change did not involve a significant hazard consideration.

As a result of subsequent discussions between the NRC Staff and the Nuclear Energy Institute on December 9, 2009, concerning information in the No Significant Hazards Consideration, Wolf Creek Nuclear Operating Corporation is providing a revised Evaluation of Proposed Change (Attachment I). Attachment I of this submittal replaces Attachment I of the Reference. The changes are indicated by a revision bar in the right margin. The final conclusions from the Regulatory Evaluation provided in the Reference remain valid and is not changed by this supplement. The submittal of this supplement was discussed with the NRC Project Manager on December 15, 2009.

In accordance with 10 CFR 50.91, a copy of this supplement is being provided to the designated Kansas State official.

This letter contains no commitments. 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,

A handwritten signature in black ink that reads "Matthew W. Sunseri". The signature is written in a cursive, slightly slanted style.

Matthew W. Sunseri

MWS/rlt

Attachment

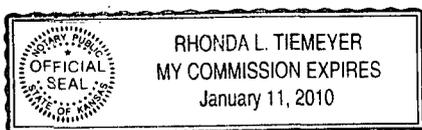
cc: E. E. Collins (NRC), w/a  
T. A. Conley (KDHE), w/a  
G. B. Miller (NRC), w/a  
B. K. Singal (NRC), w/a  
Senior Resident Inspector (NRC), w/a

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 21<sup>st</sup> day of December, 2009.



Rhonda L. Tiemeyer  
Notary Public

Expiration Date January 11, 2010

## **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," (hereafter referred to as 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**

Federal Register notice 74 FR 13926 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 10 CFR 73.1(a)(1)(v). This application requests NRC approval of the "Cyber Security Plan for Wolf Creek Nuclear Operating Corporation, Wolf Creek Generating Station," (hereafter referred to as Cyber Security Plan) in accordance with 10 CFR 73.54 and proposes changes to Section 2.E of the Renewed Facility Operating License No. NPF-42 for the Wolf Creek Generating Station (WCGS) to incorporate the provisions for implementing and maintaining in effect the provisions of the approved Cyber Security Plan. The cyber security plan is consistent with the template provided in Nuclear Energy Institute (NEI) 08-09, Revision 3, September 2009, "Cyber Security Plan for Nuclear Power Plants," and provides a description of how the requirements of the Rule will be implemented at WCGS.

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 incorporates a new requirement in the Renewed Facility Operating License to implement and maintain the Cyber Security Plan as part of the facility's overall program for physical protection. Inclusion of the Cyber Security Plan in the Renewed Facility Operating License itself does not involve any modifications to the safety related structures, systems or components (SSCs). Rather, the Cyber Security Plan describes how the requirements of 10 CFR 73.54 are to be implemented to identify, evaluate, and mitigate cyber attacks up to and including the design basis cyber attack threat, thereby achieving high assurance that the facility's digital computer and communications systems and networks are protected from cyber attacks. The implementation and incorporation of the Cyber Security Plan into the Renewed Facility Operating License will not alter previously evaluated Updated Safety Analysis Report (USAR) design basis accident analysis assumptions, add any accident initiators, or affect the function of the plant safety related SSCs as to how they are operated, maintained, modified, tested, or inspected.

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

This proposed amendment provides assurance that safety related SSCs are protected from cyber attacks. Implementation of 10 CFR 73.54 and the inclusion of the Cyber Security Plan in the Renewed Facility Operating License do not result in the need of any new or different USAR design basis accident analysis. It does not introduce new equipment that could create a new or different kind of accident, and no new equipment failure modes are created. As a result, no new accident scenarios, failure mechanisms, or limiting single failures are introduced as a result of this proposed amendment.

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 margin of safety is associated with the confidence in the ability of the fission product barriers (i.e., fuel cladding, reactor coolant pressure boundary, and containment structure) to limit the level of radiation to the public. The proposed amendment would not alter the way any safety related SSC functions and would not alter the way the plant is operated. The amendment provides assurance that safety related SSCs are protected from cyber attacks. The proposed amendment would not introduce any new uncertainties or change any existing uncertainties associated with any safety limit. The proposed amendment would have no impact

on the structural integrity of the fuel cladding, reactor coolant pressure boundary, or containment structure. Based on the above considerations, the proposed amendment would not degrade the confidence in the ability of the fission product barriers to limit the level of radiation to the public.

Therefore the proposed change does not involve a reduction in a margin of safety.

Based on the above evaluations, WCNOG 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

WCNOG 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