



June 13, 2012

Stephen E. Hedges
Site Vice President

WO 12-0045

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

- Reference: 1) Letter dated July 27, 2011, from J. R. Hall, USNRC, to M. W. Sunseri, WCNOC, "Wolf Creek Generating Station – Issuance of Amendment Re: Approval of Cyber Security Plan (TAC NO. ME 4265)"
- 2) Letter WO 11-0017, dated April 1, 2011, from S. E. Hedges, WCNOC, to USNRC

Subject: Docket No. 50-482: Revision to Cyber Security Plan Implementation Schedule Milestone

Gentlemen:

In Reference 1, the Nuclear Regulatory Commission (NRC) issued Amendment No. 197 to the Renewed Facility Operating License No. NPF-42 for Wolf Creek Generating Station (WCGS) that approved the Cyber Security Plan for Wolf Creek Nuclear Operating Corporation, Wolf Creek Generating Station (hereafter referred to as Cyber Security Plan) and associated implementation milestone schedule. The Cyber Security Plan Implementation Schedule contained in Reference 2 was utilized as part of the basis for the NRC's safety evaluation provided in Reference 1. Wolf Creek Nuclear Operating Corporation (WCNOC) is planning to implement the requirements of Implementation Milestone # 6 with a minor deviation from what was described in the approved implementation milestone schedule. Although no change to the implementation schedule dates is proposed, the changes to the description of milestone activities is conservatively considered to be a change to the Cyber Security Plan Implementation Schedule. Therefore, in accordance with the provisions of 10 CFR 50.4, "Written communications," and 10 CFR 50.90, "Application for amendment of license, construction permit, or early site permit," WCNOC is submitting a request for an amendment to the renewed facility operating license for WCGS.

SOOIA
NRK

Attachment I provides an evaluation of the proposed change. Attachment II contains proposed marked-up operating license page for the physical protection license condition for WCGS to reference the commitment change provided in this submittal. Attachment III contains the proposed revised operating license page. Attachment IV contains a change to scope of Implementation Milestone # 6. The revised commitment contained in this submittal is summarized in Attachment V.

The proposed change has been evaluated in accordance with 10 CFR 50.91(a), "Notice for public comment," using the criteria in 10 CFR 50.92, "Issuance of amendment," Section (c), and it has been determined that the change involves no significant hazards consideration. The basis for this determination is included in Attachment I.

WCNOC requests approval of the proposed amendment by December 31, 2012. It is anticipated that the license amendment, as approved, will be effective upon issuance and will be implemented within 90 days from the date of issuance.

The Plant Safety Review Committee reviewed this amendment application. In accordance with 10 CFR 50.91(b), "State consultation," 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) 364-4190, or Mr. Gautam Sen at (620) 364-4175.

Sincerely,



Stephen E. Hedges

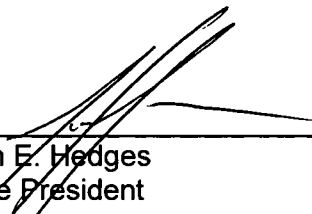
SEH/rlt

Attachment: I Evaluation of Proposed Change
II Proposed Renewed Facility Operating License Change (Mark-up)
III Retyped Renewed Facility Operating License Change
IV Revised WCNOC Cyber Security Plan Implementation Schedule
V List of Regulatory Commitments

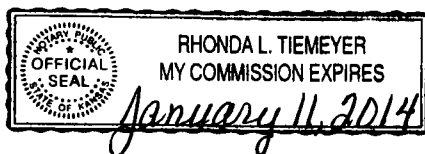
cc: E. E. Collins (NRC), w/a
T. A. Conley (KDHE), w/a
J. R. Hall (NRC), w/a
N. F. O'Keefe (NRC), w/a
Senior Resident Inspector (NRC), w/a


STATE OF KANSAS)
) SS
COUNTY OF COFFEY)

Stephen E. Hedges, of lawful age, being first duly sworn upon oath says that he is Site Vice President 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 
Stephen E. Hedges
Site Vice President

SUBSCRIBED and sworn to before me this 13th day of June, 2012.




Notary Public

Expiration Date January 11, 2014

EVALUATION OF PROPOSED CHANGE

Subject: Revision to Cyber Security Plan Implementation Schedule Milestones

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

1. SUMMARY DESCRIPTION

The proposed license amendment request includes the proposed change to an implementation schedule milestone scope and a proposed revision to the renewed facility operating license physical protection license condition (Paragraph 2.E of the Renewed Facility Operating License No. NPF-42).

2. DETAILED DESCRIPTION

In Reference 1, the Cyber Security Plan for Wolf Creek Nuclear Operating Corporation, Wolf Creek Generating Station, (hereafter referred to as Cyber Security Plan) and associated implementation schedule were approved by the Nuclear Regulatory Commission (NRC). Because the Cyber Security Plan Implementation Schedule contained in Reference 2 was utilized as a portion of the basis for the NRC's safety evaluation provided by Reference 1, this proposed amendment request includes: 1) a proposed change to the existing renewed facility operating license condition for the physical protection license condition to reference a deviation for an implementation schedule milestone and 2) a proposed Revised Cyber Security Plan Implementation Schedule for the scope of Implementation Milestone # 6. Implementation Milestone # 6 requires the identification, documentation, and implementation of cyber security controls for critical digital assets (CDAs) that could adversely impact the design function of physical security target set equipment by no later than December 31, 2012. This change provides a deviation to the scope of Implementation Milestone # 6 to apply only to technical cyber security controls.

Implementation Milestone # 6 currently states, in part:

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.

The milestone is revised (changes shown in italics) to state, in part:

Identify, document, and implement *NEI 08-09, Revision 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 *target set* CDAs that could adversely impact the design function of physical security target set equipment.

3. TECHNICAL EVALUATION

In Reference 3, the Nuclear Energy Institute (NEI) transmitted to the NRC an implementation schedule template to aid compliance with the NRC's cyber security regulations codified in 10 CFR 73.54 which was acknowledged in Reference 4 by the NRC. NEI engaged the industry in an effort to ensure that utilities submit an implementation schedule consistent with the template provided by Reference 3. Wolf Creek Nuclear Operating Corporation (WCNOC) provided the requested implementation schedule in Reference 2 in accordance with the template which the NRC acknowledged in Reference 4.

During the industry's efforts to submit implementation schedules, several other utilities changed, via deviation, the Implementation Milestone # 6 scope. Implementation Milestone # 6 of the template regards the identification, documentation, and implementation of cyber security controls for critical digital assets (CDAs) by December 31, 2012. The other utilities Milestone # 6 deviation was to change the scope of cyber security controls to be addressed to include only the NEI 08-09, Revision 6 (Reference 5), Appendix D, technical controls excluding the operational and management controls on the basis that implementing the technical controls for target set CDAs provides a high degree of protection against cyber-related attacks that could lead to radiological sabotage. Furthermore, these other utilities justified that existing programs that are currently in place (e.g., physical protection, maintenance and work management, configuration management, and operational experience, etc.) provide a high degree of operational and management protection during the interim period until such time that the full Cyber Security Program is implemented. The NRC found the deviations to Milestone # 6 scope for other utilities to be acceptable, and issued Safety Evaluations to plants whose implementation schedule incorporated the deviation. Precedent is cited in Section 4.2.

In Reference 2, WCNOG previously submitted the implementation schedule without articulating the deviation to the scope of Implementation Milestone # 6. Implementation Milestone # 6 with the deviation focuses the efforts on the application of technical cyber security controls to those CDAs that are part of a target set or could impact the proper functioning of target set equipment. Based on the above justification and the fact that the NRC has already approved such deviation for several other utilities, WCNOG is requesting this license amendment in order to specify that the cyber security controls being identified, documented, and implemented in Implementation Milestone #6 are the technical cyber security controls and existing plant programs are sufficient to satisfy the Implementation Milestone #6 operational and management controls referenced in the Cyber Security Plan.

In conclusion, existing programs at WCGS currently in place (e.g., physical protection, maintenance and work management, configuration management, and operational experience, etc.) provide sufficient operational and management protection during the interim period until such time that the full Cyber Security Program is implemented. The cyber security controls to be identified, documented, and implemented in Implementation Milestone # 6 of the Revised WCNOG Cyber Security Plan Implementation Schedule (Attachment IV) are the technical cyber security controls with the exception of the operational and management controls referenced in the Cyber Security Plan that will be completed following evaluation of the remaining CDAs and implemented with full Cyber Security Program implementation.

This license amendment request includes the proposed change to the existing renewed facility operating license condition for physical protection (Attachments II and III) for WCGS. The license amendment request contains the proposed Revised WCNOG Cyber Security Plan Implementation Schedule (Attachment IV).

4. REGULATORY EVALUATION

4.1 Applicable Regulatory Requirements/Criteria

10 CFR 73.54 requires licensees to maintain and implement a cyber security plan. Wolf Creek Generating Station (WCGS) renewed facility operating license includes a physical protection license condition (Paragraph 2.E of the Renewed Facility Operating License No. NPF-42) that

requires Wolf Creek Nuclear Operating Corporation (WCNOC) to fully implement and maintain in effect all provisions of the Commission-approved cyber security plan, including changes made pursuant to the authority of 10 CFR 50.90 and 10 CFR 50.54(p).

4.2 Precedent

Amendment No. 203 (Reference 6) approved an implementation schedule using the NEI template (Reference 3), with the exception of Milestone 6 for the Callaway Plant. The Callaway Plant deviated from the template for Milestone 6 to address only the NEI 08-09, Revision 6, Appendix D technical controls, excepting for the operational and management controls, on the basis that implementing the technical controls for the target set CDAs provides a high degree of protection against cyber related attacks that could lead to radiological sabotage.

The changes being proposed by WCNOC in this amendment request are similar to those approved in the Callaway Plant Amendment No. 203.

4.3 No Significant Hazards Consideration

WCNOC is requesting an amendment to the Renewed Facility Operating License No. NPF-42 to revise the physical protection license condition (Paragraph 2.E) as it relates to the cyber security plan. This change includes a proposed deviation to the scope of the WCNOC Cyber Security Plan Implementation Schedule milestone and a proposed revision to Paragraph 2.E of the renewed facility operating license to include the proposed deviation. Specifically, WCNOC proposes a deviation to the scope of Implementation Milestone # 6 to apply to only technical cyber security controls.

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. Does the proposed change involve a significant increase in the probability or consequences of an accident previously evaluated?

Response: No

The proposed change to the WCNOC Cyber Security Plan Implementation Schedule is administrative in nature. This change does not alter accident analysis assumptions, add any initiators, or affect the function of plant systems or the manner in which systems are operated, maintained, modified, tested, or inspected. The proposed change does not require any plant modifications which affect the performance capability of the structures, systems, and components (SSCs) relied upon to mitigate the consequences of postulated accidents, and has 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. Does the proposed change create the possibility of a new or different kind of accident from any accident previously evaluated?

Response: No

The proposed change to the WCNOG Cyber Security Plan Implementation Schedule is administrative in nature. This proposed change does not alter accident analysis assumptions, add any initiators, or affect the function of plant systems or the manner in which systems are operated, maintained, modified, tested, or inspected. The proposed change does not require any plant modifications which affect the performance capability of the SSCs relied upon to mitigate the consequences of postulated accidents, and does not create the possibility of a new or different kind of accident from any accident previously evaluated.

Therefore, the proposed change does not create the possibility of a new or different kind of accident from any previously evaluated.

3. Does the proposed change involve a significant reduction in a margin of safety?

Response: No

Plant safety margins are established through limiting conditions for operation, limiting safety system settings, and safety limits specified in the technical specifications. The proposed change to the WCNOG Cyber Security Plan Implementation Schedule is administrative in nature. Since the proposed change is administrative in nature, there is no change to these established safety margins.

Therefore the proposed change does not involve a significant 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.

4.4 Conclusions

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) and (12). Therefore, pursuant to 10 CFR 51.22(b), an environmental assessment of the proposed change is not required.

6. REFERENCES

1. NRC letter from J. R. Hall, USNRC, to M. W. Sunseri, WCNOC, "Wolf Creek Generating Station – Issuance of Amendment Re: Approval of Cyber Security Plan (TAC NO. ME4265)," July 27, 2011. (ADAMS Accession No. ML111990339)
2. WCNOC letter WO 11-0017, "Response to Request for Additional Information Regarding License Amendment Request for Approval of the Cyber Security Plan," April 1, 2011. (ADAMS Accession No. ML110970134)
3. Letter from C. E. Earls, NEI, to R. P. Correia, USNRC, "Template for the Cyber Security Plan Implementation Schedule," dated February 28, 2011. (ADAMS Accession No. ML110600211)
4. Letter from R. P. Correia, USNRC, to C. E. Earls, NEI, "Template for the Cyber Security Plan Implementation Schedule," dated March 1, 2011. (ADAMS Accession No. ML110070348)
5. NEI 08-09, "Cyber Security Plan for Nuclear Power Reactors," Revision 6, April 2010.
6. NRC letter from M. C. Thadani, USNRC, to A. C. Heflin, Union Electric Company, "Callaway Plant, Unit 1 – Issuance of Amendment Re: Approval of Cyber Security Plan (TAC NO. ME4536)," August 17, 2011. (ADAMS Accession No. ML112140087)

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.

The licensee shall fully implement and maintain in effect all provisions of the Commission-approved cyber security plan (CSP), including changes made pursuant to the authority of 10 CFR 50.90 and 10 CFR 50.54(p). The licensee's CSP was approved by License Amendment No. 197⁶

- F. Deleted per Amendment No. 141.

, as supplemented by a change approved by License Amendment No. XXX.

- 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, WCNOG may make changes to the programs and activities described in the supplement without prior Commission approval, provided that WCNOG evaluates such changes pursuant to the criteria set forth in 10 CFR 50.59 and otherwise complies with the requirements in that section.

Renewed License No. NPF-42
Amendment No. 479, 197

RETYPED 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 (CSP), including changes made pursuant to the authority of 10 CFR 50.90 and 10 CFR 50.54(p). The licensee's CSP was approved by License Amendment No. 197, as supplemented by a change approved by License Amendment No. xxx.
- 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, WCNOG may make changes to the programs and activities described in the supplement without prior Commission approval, provided that WCNOG evaluates such changes pursuant to the criteria set forth in 10 CFR 50.59 and otherwise complies with the requirements in that section.

REVISED WCNOC CYBER SECURITY PLAN IMPLEMENTATION SCHEDULE

#	Implementation Milestone	Completion Date	Basis
6	<p>Identify, document, and implement NEI 08-09, Revision 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 target set 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	<p>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 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.</p> <p><u>Note</u> that the Operational and Management controls, as provided in NEI 08-09, Rev. 6, Appendix E, will be implemented in conjunction with the full implementation of the Cyber Security Program. These controls are primarily procedure based programs and must be implemented in coordination with the comprehensive Cyber Security Program. However, a high degree of protection against cyber related attacks is maintained as many of these programs (e.g., physical protection, maintenance and work management, configuration management, operational experience, etc) are currently in place and are well established within the nuclear industry.</p>

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. Gautam Sen at (620) 364-4175.

Regulatory Commitments	Due Date / Event
Identify, document, and implement NEI 08-09, Revision 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 target set CDAs that could adversely impact the design function of physical security target set equipment.	December 31, 2012