WOLF CREEK
NUCLEAR OPERATING CORPORATION

Cleveland Reasoner
Site Vice President

June 14, 2016

WO 16-0023

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

References: 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. ME4265)"

2) Memorandum dated October 24, 2013, from R. Felts, USNRC to B. Westreich, USNRC, "Review Criteria for Title 10 of the Code of Federal Regulations Part 73.54, Cyber Security Implementation Schedule Milestone 8 License Amendment Requests"

3) Letter dated August 14, 2014, from C. F. Lyon, USNRC to A. C. Heflin, WCNOC, "Wolf Creek Generating Station – Issuance of Amendment Re: Revision to Cyber Security Plan Implementation Schedule Completion Date (TAC No. MF3392)"

Subject: Docket No. 50-482: License Amendment Request (LAR) for Revision to the Cyber Security Plan Implementation Schedule Completion Date

Gentlemen:

Pursuant to 10 CFR 50.90, "Application for amendment of license, construction permit, or early site permit," Wolf Creek Nuclear Operating Corporation (WCNOC) hereby requests an amendment to Renewed Facility Operating License No. NPF-42 for the Wolf Creek Generating Station (WCGS). In accordance with the guidelines provided by Reference 2, this request proposes a change to the Cyber Security Plan for Wolf Creek Nuclear Operating Corporation, Wolf Creek Generating Station Milestone 8 full implementation date as set forth in the Cyber Security Plan Implementation Schedule approved by Reference 1 and amended by Reference 3.

Attachment I provides an evaluation and justification for the proposed change. Attachment II contains the proposed marked-up operating license page for the physical protection license condition for WCGS to reference the commitment change provided in this submittal. Attachment

SD01A
NRR

III contains the proposed revised operating license page. Attachment IV contains a revised Cyber Security Plan Implementation Schedule which includes a change to the completion date for Implementation Milestone 8. Attachment V contains one revised commitment related to the full implementation of the Cyber Security Plan for Wolf Creek Nuclear Operating Corporation, Wolf Creek Generating Station.

It has been determined that this amendment application does not involve a significant hazard consideration as determined per 10 CFR 50.92, "Issuance of amendment." The basis for this determination is included in Attachment I. Pursuant to 10 CFR 51.22, "Criterion for categorical exclusion; identification of licensing and regulatory actions eligible for categorical exclusion or otherwise not requiring environmental review," Section (b), no environmental impact statement or environmental assessment needs to be prepared in connection with the issuance of this amendment.

The Plant Safety Review Committee reviewed this amendment application. In accordance with 10 CFR 50.91, "Notice for public comment; State consultation," a copy of this amendment application, with attachments is being provided to the designated Kansas State official.

WCNOC requests review and approval of the proposed amendment by May 1, 2017. It is anticipated that the license amendment, as approved, will be effective upon issuance and will be implemented within 30 days from the date of issuance.

If you have any questions concerning this matter, please contact me at (620) 364-4171, or Cynthia R. Hafenstine (620) 364-4204.

Sincerely,

Cleveland Reasoner

COR/rlt

Attachments: I Evaluation of Proposed Change
II Proposed Markup of Renewed Facility Operating License Page
III Revised Renewed Facility Operating License Page
IV Revised Cyber Security Plan Implementation Schedule
V List of Regulatory Commitments

cc: M. L. Dapas (NRC), w/a
C. F. Lyon (NRC), w/a
K. S. Steves (KDHE), w/a
N. H. Taylor (NRC), w/a
Senior Resident Inspector (NRC), w/a

STATE OF KANSAS)
) SS
COUNTY OF COFFEY)

Cleveland Reasoner, 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 _____
Cleveland Reasoner
Site Vice President

SUBSCRIBED and sworn to before me this 14th day of June, 2016.

STATE OF KANSAS NOTARY PUBLIC
RHONDA L. TIEMEYER
My Appointment Expires
January 11, 2018

_____
Notary Public

Expiration Date January 11, 2018

EVALUATION OF PROPOSED CHANGE

License Amendment Request for Revision to the Wolf Creek Nuclear Operating Corporation Cyber Security Plan Implementation Schedule (Milestone 8) Completion Date

1.0 SUMMARY DESCRIPTION

This license amendment request includes a proposed change to the Cyber Security Plan for Wolf Creek Nuclear Operating Corporation, Wolf Creek Generating Station (hereafter referred to as Cyber Security Plan) Implementation Schedule Milestone 8 and a proposed revision to the renewed facility operating license physical protection license condition contained in Paragraph 2.E of the Wolf Creek Generating Station (WCGS) Renewed Facility Operating License No. NPF-42).

2.0 DETAILED DESCRIPTION

In Reference 1, the Nuclear Regulatory Commission (NRC) provided criteria to be used for evaluation of a license amendment request to revise the Cyber Security Plan Implementation Schedule Milestone 8 date. In Reference 2, the NRC issued a license amendment that approved the Wolf Creek Nuclear Operating Corporation (WCNOC) Cyber Security Plan and associated implementation schedule. 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 2. In Reference 3, the NRC issued a license amendment that approved a revised implementation schedule. Implementation Milestone 8 currently requires WCNOC fully implement the Cyber Security Plan for all applicable safety, security, and emergency preparedness (SSEP) functions by no later than June 30, 2017. WCNOC is now proposing a change to the Implementation Milestone 8 date for full implementation of the Cyber Security Plan for all SSEP functions.

The completion date for Implementation Milestone 8 is currently:

June 30, 2017

The completion date is revised to:

December 31, 2017

3.0 TECHNICAL EVALUATION

In Reference 2, the NRC approved WCNOC's Cyber Security Plan and associated implementation schedule. This schedule consists of eight milestones, with interim Milestones 1 through 7 being completed by December 31, 2012, and Milestone 8 (full compliance) to be completed by December 15, 2014. During the process of accomplishing Interim Milestones 1 through 7 and commencing Milestone 8 work, it became evident to WCNOC that additional time would be required, and a schedule extension request to June 30, 2017 was approved by the NRC (Reference 3). However, it has subsequently become evident that an additional extension is necessary. The extension requested herein is for an Implementation Milestone 8 date of December 31, 2017.

An NRC memorandum (Reference 1) provides eight criteria for the review of license amendment requests to revise implementation schedule Milestone 8 dates. These criteria serve to explain the current status of the WCNOC cyber security program and the need for the Implementation Milestone 8 completion date revision.

Below is WCNOC's discussion of the eight evaluation criteria provided by Reference 1:

1) Identification of the specific requirements of the cyber security plan that WCNOC needs additional time to implement.

The Cyber Security Plan Sections 3 and 4 describe requirements for application and maintenance of cyber security controls listed in Appendices D and E of Nuclear Energy Institute (NEI) 08-09, Revision 6, "Cyber Security Plan for Nuclear Power Reactors" (Reference 4). Application of the controls is accomplished after completion of detailed analyses (the cyber security assessment process) that identify "gaps," or the difference between current configuration and a configuration that satisfies each cyber security control. Gap closure can require any combination of physical, logical (software-related), or programmatic/procedural changes. Specific requirements needing additional time include:

a. WCNOC is in the process of determining the need and implementation for automated security information and event management (SIEM) systems and designing/implementing these systems for monitoring activity on networks of critical digital assets (CDAs), pursuant to NEI 08-09, Revision 6, Appendix D-2, and Appendices E-3.4, 3.5, and 4.3.

b. Additional physical controls for CDAs outside the security protected area pursuant to NEI 08-09, Revision 6, Appendix E-5.1.

c. Significant programmatic change management associated with approximately 50 procedure changes pursuant to NEI 08-09, Revision 6, Appendix E.

2) Detailed justification that describes the reason WCNOC requires additional time to implement the specific requirements identified.

a. During October of 2015, the NRC completed an inspection of WCNOC's compliance with interim Milestones 1 through 7. The preparation for and support of these inspections has required a significant commitment of time from WCNOCs most knowledgeable subject matter experts on nuclear cyber security, exceeding the estimate previously developed and therefore, drawing those resources away from Milestone 8 implementation activities.

b. Development of an endorsed written standard for interpreting and applying NEI 08-09 cyber security controls has continued to be a work-in-progress. NEI 13-10, "Cyber Security Control Assessments," (Reference 5) is a guideline intended to provide some reduction of controls implementation based on equipment safety significance. Revision 3 of NEI 13-10 was endorsed by the NRC in September, 2015, followed by Revision 4 which was endorsed by the NRC in December, 2015. Prior to the changes incorporated in Revision 3 of NEI 13-10, an intial screening of WCGS CDAs using this guideline indicated the reduction in both analytical work and actual application of controls was not significant. The release of Revision 3 of NEI 13-10, and then subsequently, Revision 4 appears to provide some reduction in level of effort but more time is needed to take full advantage of the guidance.

c. In June 2014, NEI submitted a petition for rulemaking to the Commission. The petition was subsequently found acceptable for review. The petition proposes a change to the rule to more precisely align the scope of the rule with the underlying objective of preventing radiological sabotage, which NEI estimates could potentially result in a

reduction in the scope of cyber security implementation. While WCNOC does not intend to suspend any implementation work in anticipation of the petition being approved, the petition being submitted is indicative that the final process for implementing the rule has not been stabilized, and therefore, WCNOC requires additional time to receive any implementation benefit from such rulemaking.

d. Benchmarking data gathered on Milestone 8 implementation schedules for other licensees indicate that a significant number of licensees have either gained approval or have submitted an extension request for a new Milestone 8 date in December of 2017. Therefore, WCNOC's request is consistent with the industry.

e. The following items also contribute to the need for additional time to implement Milestone 8:

- Resolution of ongoing NEI/NRC discussion on CDA scope/security controls as well as requested clarifications on industry guidance provided within NEI 08-09 Revision 6 and NEI 13-10 Revision 4
- Defining the cyber security controls in NEI 08-09 Revision 6 is resource intensive and without guidance for what "good" looks like for each control there is high risk of rework as industry interpretation change
- CDA mitigation activities defined in Section 3.1.6 of the Cyber Security Plan are resource intensive
- Remediation activities need to be carefully considered
- Change management challenges
- Training on new programs, processes and procedures

3) A proposed completion date for Milestone 8 consistent with the remaining scope of work to be conducted and the resources available.

WCNOC is requesting a change to the Implementation Milestone 8 completion date from June 30, 2017 to December 31, 2017 to complete CDA assessments, implement design modifications based on assessment results, update existing procedures, develop new program procedures and provide training to complete full implementation of the cyber security program.

4) An evaluation of the impact that the additional time to implement the requirements will have on the effectiveness of WCNOC's overall cyber security program in the context of milestones already completed.

The impact of the requested additional implementation time on the effectiveness of the overall cyber security program is considered to be very low because WCNOC has completed the interim Implementation Milestones 1 through 7 required by December 31, 2012 and the "Good Faith Letter" (Reference 6) required actions by October 29, 2013. The completed activities provide a high degree of protection against cyber attacks while WCNOC implements the full program. The completed activities include:

a. A WCNOC Cyber Security Assessment Team (CSAT) has been implemented consisting of highly experienced personnel knowledgeable in reactor and balance-of-plant design, licensing, safety, security, emergency preparedness, information technology, and cyber security. The CSAT is provided with the authority, via written procedure, to perform the analyses and oversight activities described in the Cyber Security Plan.

b. Critical systems and CDAs have been identified, documented, and entered into the WCNOC records system.

c. The plant process computer network and the plant security computer network have been deterministically isolated per the requirements of cyber security Interim Milestone 3.

d. Safety-related, important-to-safety, and security CDAs have been extensively reviewed and verified (or modified) to be deterministically isolated and not to employ wireless technology.

e. Procedures have been implemented for portable digital media and devices periodically connected to CDAs, per NEI 08-09, Revision 6, Appendix D, Section 1.19.

f. CDAs associated with physical security target sets have been analyzed per the requirements of the CSP Section 3.1.6 and verified to satisfy the technical cyber security controls described in NEI 08-09, Revision 6, Appendix D.

g. Employees have been provided with training on cyber security awareness, tampering, and control of portable digital media and devices periodically connected to CDAs.

h. WCNOC has transitioned from the previous cyber security program described by NEI 04-04. Revisions have been made to procedures that control plant modifications, planning, and maintenance, establishing ties to cyber security procedures for CDA analysis and control of portable digital media and devices periodically connected to CDAs.

5) A description of WCNOC's methodology for prioritizing completion of work for critical digital assets associated with significant safety, security, or emergency preparedness consequences and with reactivity effects in the balance of plant.

WCNOC methodology for prioritizing Implementation Milestone 8 activities is centered on considerations for SSEP and Balance of Plant (BOP) continuity of power consequences. The methodology is based on defense-in-depth, installed configuration of the CDAs and susceptibility to the five commonly identified threat vectors listed in the NRC Cyber Security Significance Determination Process. Prioritization for CDA assessment begins with safety related CDAs and continues through the lower priority non-safety and emergency preparedness (EP) CDAs:

- Safety related CDAs
- Physical security CDAs
- Important to safety CDAs (including BOP CDAs that directly impact continuity of power) and control system CDAs
- Non-safety related CDAs and EP CDAs

The remainder of the Implementation Milestone 8 work will be fully implemented by the revised December 31. 2017 completion date including:

- The balance of the non-safety related and EP CDA assessments
- Completion of all individual security control design remediation actions including those that require a refueling outage for implementation
- Completion of station procedure revisions (50 plus) to integrate the cyber security program
- Integration of on-going periodic and time based actions into the plant preventative maintenance/surveillance (or equivalent) programs

- Complete implementation of the cyber security change management plan including any required training

6) A discussion of WCNOC's cyber security program performance up to the date of the license amendment request.

A Quality Assurance (QA) surveillance of interim Implementation Milestones 1 through 7 has concluded that WCNOC has an effective program an additional on-going QA surveillances under the physical and cyber security programs will be conducted during the interim period. Audit/assessment issues are entered into the Corrective Action Program (CAP) and addressed for program improvement.

In October 2015, the NRC completed an inspection related to compliance with interim Milestones 1 through 7. All findings were found to meet the criteria described in the Reference 6 for enforcement discretion, and were entered into the CAP.

On-going monitoring and time-based periodic actions provide continuing program performance monitoring.

7) A discussion of cyber security issues pending in WCNOC's corrective action program.

There are presently no significant (constituting a threat to a CDA via cyber means or calling into question program effectiveness) nuclear cyber security issues pending in the CAP. Several non-significant issues identified during the recent NRC inspection described above have been entered into the CAP. All outstanding items associated with the Milestone 1-7 NRC inspection are being tracked in accordance with the WCNOC CAP.

8) A discussion of modifications completed to support the cyber security program and a discussion of pending cyber security modifications.

Modifications completed include installation of modifications associated with Milestone 3 in accordance with the Cyber Security Plan and associated defense in depth procedures.

Pending modifications which will be completed prior to the revised December 31, 2017 date include:

- Cyber hardening of turbine control and turbine supervisory system
- Cyber hardening of plant process computer system
- Cyber hardening of plant security system
- Installation of centralized monitoring system

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. This license amendment request also contains the proposed revised WCNOC Cyber Security Plan Implementation Schedule (Attachment IV). A revised list of regulatory commitments is also provided (Attachment V).

4.0 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 No. NPF-42 includes a physical protection license condition 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 No Significant Hazards Consideration Determination

Pursuant to 10 CFR 50.90, "Application for amendment of license, construction permit, or early site permit," WCNOC hereby requests an amendment to the Renewed Facility Operating License No. NPF-42 for WCGS. This amendment request proposes a change to the Implementation Milestone 8 completion date specified in the WCNOC Cyber Security Plan Implementation Schedule.

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 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 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 WCNOC 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 systems settings, and safety limits specified in the technical specifications. The proposed change to the WCNOC Cyber Security Plan Implementation Schedule is administrative in nature. Since the proposed change is administrative in nature, there are no changes 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, 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

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.

5.0 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 a significant increase in the amounts of any effluent that may be released offsite, or (iii) a significant increase in individual or cumulative occupational radiation exposure. Accordingly, the proposed change meets the eligibility criterion for categorical exclusion set forth in 10 CFR 51.22(c)(12). Therefore, pursuant to 10 CFR 51.22(b) no environmental impact statement or environmental assessment need be prepared in connection with the proposed amendment.

6.0 REFERENCES

1. NRC Memorandum from R. Felts, USNRC to B. Westreich, USNRC, "Review Criteria for Title 10 of the Code of Federal Regulations Part 73.54, Cyber Security Implementation Schedule Milestone 8 License Amendment Requests," October 24, 2013. ADAMS Accession No. ML13295A467.

2. 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.

3. NRC Letter from C. F. Lyon, USNRC, to A. C. Heflin, WCNOC, "Wolf Creek Generating Station – Issuance of Amendment Re: Revision to Cyber Security Plan Implementation Schedule Completion Date (TAC No. MF3392)," August 14, 2014. ADAMS Accession No. ML14209A023.

4. NEI 08-09, "Cyber Security Plan for Nuclear Power Reactors," Revision 6, April 2010.

5. NEI 13-10, "Cyber Security Control Assessments," Revision 3, September 2015; Revision 4, November 2015.

6. NRC Memorandum from B. Westreich, USNRC, to T. Blount, USNRC, "Enhanced Guidance for Licensee Near-Term Corrective Actions to Address Cyber Security Inspection Findings and Licensee Eligibility for 'Good-Faith' Attempt Discretion," July 1, 2013. ADAMS Accession ML13178A203.

PROPOSED MARK-UP OF RENEWED FACILITY OPERATING LICENSE PAGE

(16) Additional Conditions

The Additional Conditions contained in Appendix D, as revised through Amendment No. 179, 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 changes approved by License Amendment No. 202, ~~and~~ License Amendment No. 210~~.~~ , and 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, 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.

REVISED RENEWED FACILITY OPERATING LICENSE PAGE

(16) Additional Conditions

The Additional Conditions contained in Appendix D, as revised through Amendment No. 179, 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 changes approved by License Amendment No. 202, License Amendment No. 210, and License Amendment No.

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.

REVISED CYBER SECURITY PLAN IMPLEMENTATION SCHEDULE

#	Implementation Milestone	Completion Date	Basis
8	Full implementation of the WCNOC Cyber Security Plan for all SSEP functions will be achieved.	December 31, 2017	By the completion date, the WCNOC Cyber Security Plan will be fully implemented for all SSEP functions in accordance with 10 CFR 73.54. This date also bounds the completion of all individual asset security control design remediation actions including those that require a refuel outage for implementation. The full implementation date includes the addition into scope of the Balance of Plant (BOP) SSCs that could directly or indirectly affect reactivity.

LIST OF REGULATORY COMMITMENTS

The following table identifies those actions committed to by WCNOC 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 Cynthia Hafenstine at (620) 364-4204.

Regulatory Commitments	**Due Date/ Event**
Fully implement the Cyber Security Plan for all SSEP functions.	December 31, 2017