UNITED STATES
NUCLEAR REGULATORY COMMISSION
WASHINGTON, D.C. 20555-0001

March 24, 2017

Mr. Adam C. Heflin
President, Chief Executive Officer,
and Chief Nuclear Officer
Wolf Creek Nuclear Operating Corporation
P.O. Box 411
Burlington, KS 66839

SUBJECT: WOLF CREEK GENERATING STATION - ISSUANCE OF AMENDMENT RE: REVISION TO THE CYBER SECURITY PLAN IMPLEMENTATION SCHEDULE (CAC NO. MF7998)

Dear Mr. Heflin:

The U.S. Nuclear Regulatory Commission (NRC, the Commission) has issued the enclosed Amendment No. 217 to Renewed Facility Operating License No. NPF-42 for the Wolf Creek Generating Station (WCGS). The amendment consists of changes to the facility operating license in response to your application dated June 14, 2016.

The amendment approves the revised schedule for full implementation of the cyber security plan (CSP) from June 30, 2017, to December 31, 2017, and revises paragraph 2.E of Renewed Facility Operating License No. NPF-42 for WCGS, to incorporate the revised CSP implementation schedule.

A copy of our related Safety Evaluation is enclosed. The Notice of Issuance will be included in the Commission's next biweekly *Federal Register* notice.

Sincerely,

Balwant K. Singal, Senior Project Manager
Plant Licensing Branch IV
Division of Operating Reactor Licensing
Office of Nuclear Reactor Regulation

Docket No. 50-482

Enclosures:
1. Amendment No. 217 to NPF-42
2. Safety Evaluation

cc w/encls: Distribution via Listserv

SUBJECT: WOLF CREEK GENERATING STATION - ISSUANCE OF AMENDMENT RE: REVISION TO THE CYBER SECURITY PLAN IMPLEMENTATION SCHEDULE (CAC NO. MF7998) DATED MARCH 24, 2017

DISTRIBUTION:

PUBLIC	RidsNrrLAPBlechman Resource	JRycyna, NSIR/CSD
LPL4 r/f	RidsNrrPMWolfCreek Resource	
RidsACRS_MailCTR Resource	RidsRgn4MailCenter Resource	
RidsNrrDorlLpl4 Resource	RidsNsirCsd Resource	

***via memo dated January 5, 2017**
****per email dated March 21, 2017**

ADAMS Accession No. ML17024A241

OFFICE	NRR/DORL/LPL4/PM	NRR/DORL/LPL4/LA	NSIR/CSD/DD
NAME	BSingal	PBlechman w/comments	JBeardsley*
DATE	02/06/17	02/06/17	01/05/17
OFFICE	OGC /NLO	NRR/DORL/LPL4/BC	NRR/DORL/LPL4/PM
NAME	NStAmour**	RPascarelli	BSingal
DATE	03/21/17	03/24/17	03/24/17

OFFICIAL RECORD COPY

UNITED STATES
NUCLEAR REGULATORY COMMISSION
WASHINGTON, D.C. 20555-0001

WOLF CREEK NUCLEAR OPERATING CORPORATION

WOLF CREEK GENERATING STATION

DOCKET NO. 50-482

AMENDMENT TO RENEWED FACILITY OPERATING LICENSE

Amendment No. 217
License No. NPF-42

1. The Nuclear Regulatory Commission (the Commission) has found that:

   A. The application for amendment to the Wolf Creek Generating Station (the facility) Renewed Facility Operating License No. NPF-42 filed by the Wolf Creek Nuclear Operating Corporation (the Corporation), dated June 14, 2016, complies with the standards and requirements of the Atomic Energy Act of 1954, as amended (the Act), and the Commission's rules and regulations set forth in 10 CFR Chapter I;

   B. The facility will operate in conformity with the application, as amended, the provisions of the Act, and the rules and regulations of the Commission;

   C. There is reasonable assurance (i) that the activities authorized by this amendment can be conducted without endangering the health and safety of the public, and (ii) that such activities will be conducted in compliance with the Commission's regulations;

   D. The issuance of this license amendment will not be inimical to the common defense and security or to the health and safety of the public; and

   E. The issuance of this amendment is in accordance with 10 CFR Part 51 of the Commission's regulations and all applicable requirements have been satisfied.

2. Accordingly, the license is amended by changes as indicated in the attachment to this license amendment and paragraph 2.E of Renewed Facility Operating License No. NPF-42 is hereby amended to read, in part, as follows:

> 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. 217.

3. The license amendment is effective as of its date of issuance and shall be implemented within 30 days of the date of issuance. The full implementation of CSP shall be in accordance with the implementation schedule submitted by the licensee on June 14, 2016, and approved by the NRC staff with this license amendment. All subsequent changes to the NRC-approved CSP implementation schedule will require NRC approval pursuant to 10 CFR 50.90.

FOR THE NUCLEAR REGULATORY COMMISSION

Robert J. Pascarelli, Chief
Plant Licensing Branch IV
Division of Operating Reactor Licensing
Office of Nuclear Reactor Regulation

Attachment:
Changes to the Renewed Facility
Operating License

Date of Issuance: March 24, 2017

ATTACHMENT TO LICENSE AMENDMENT NO. 217 TO

RENEWED FACILITY OPERATING LICENSE NO. NPF-42

WOLF CREEK GENERATING STATION

DOCKET NO. 50-482

Replace the following page of the Renewed Facility Operating License No. NPF-42 with the attached revised page. The revised page is identified by amendment number and contains a marginal line indicating the area of change.

Renewed Facility Operating License

REMOVE	INSERT
7	7

(16) Additional conditions

The Additional Conditions contained in Appendix D, as revised through Amendment No. 213, 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. 217.

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.

UNITED STATES
NUCLEAR REGULATORY COMMISSION
WASHINGTON, D.C. 20555-0001

SAFETY EVALUATION BY THE OFFICE OF NUCLEAR REACTOR REGULATION

RELATED TO AMENDMENT NO. 217 TO

RENEWED FACILITY OPERATING LICENSE NO. NPF-42

WOLF CREEK NUCLEAR OPERATING CORPORATION

WOLF CREEK GENERATING STATION

DOCKET NO. 50-482

1.0 INTRODUCTION

By letter dated June 14, 2016 (Agencywide Documents Access and Management System (ADAMS) Accession No. ML16174A121), Wolf Creek Nuclear Operating Corporation (WCNOC, the licensee) requested a change to the renewed facility operating license for the Wolf Creek Generating Station (WCGS).

The U.S. Nuclear Regulatory Commission (NRC) staff initially reviewed and approved the licensee's Cyber Security Plan (CSP) implementation schedule by Amendment No.197 dated July 27, 2011 (ADAMS Accession No. ML 111990339). Subsequently, the NRC staff reviewed and approved Amendment No. 201, dated December 12, 2012 (ADAMS Accession No. ML12279A250), to modify Milestone 6 to change the scope of the cyber security controls to be implemented by the committed date, and Amendment No. 210, dated August 14, 2014 (ADAMS Accession No. ML14209A023), which extended the CSP implementation schedule. The schedule approved by Amendment No. 210 required WCGS to fully implement and maintain all provisions of the CSP by June 30, 2017.

The proposed change would revise the date of CSP Implementation Schedule Milestone 8 and paragraph 2.E in the renewed facility operating license from June 30, 2017 to December 31, 2017. Milestone 8 of the CSP implementation schedule concerns the full implementation of the CSP. The NRC issued a proposed finding that the amendment involves no significant hazards consideration, published in the *Federal Register* on August 16, 2016 (81 FR 54618).

2.0 REGULATORY EVALUATION

The NRC staff reviewed and approved the licensee's existing CSP implementation schedule by letter dated August 14, 2014, Amendment No. 210 to Renewed Facility Operating License No. NPF-42 for WCGS. The NRC staff considered the following regulatory requirements and guidance in its review of the license amendment request (LAR) to modify the existing CSP implementation schedule:

- Title 10 of the *Code of Federal Regulations* (10 CFR), Section 73.54, "Protection of digital computer and communication systems and networks," which states, in part:

> Each [CSP] submittal must include a proposed implementation schedule. Implementation of the licensee's cyber security program must be consistent with the approved schedule.

- The licensee's renewed facility operating license includes a license condition that requires the licensee to fully implement and maintain in effect all provisions of the Commission-approved CSP.

- Review criteria provided by the NRC staff's internal memorandum, "Review Criteria for Title 10 of the *Code of Federal Regulations* Part 73.54, Cyber Security Implementation Schedule Milestone 8 License Amendment Requests," dated October 24, 2013 (ADAMS Accession No. ML13295A467), to be considered for evaluating licensees' requests to postpone their cyber security program implementation date (commonly known as Milestone 8).

The NRC staff does not regard the CSP milestone implementation dates as regulatory commitments that can be changed unilaterally by the licensee, particularly in light of the regulatory requirement at 10 CFR 73.54, that states, in part, that "[i]mplementation of the licensee's cyber security program must be consistent with the approved schedule." As the NRC staff explained in its letter to all operating reactor licensees dated May 9, 2011 (ADAMS Accession No. ML110980538), the implementation of the plan, including the key intermediate milestone dates and the full implementation date shall be in accordance with the implementation schedule submitted by the licensee and approved by the NRC. All subsequent changes to the NRC-approved CSP implementation schedule, thus, will require prior NRC approval as required by 10 CFR 50.90, "Application for amendment of license, contruction permit, or early site permit."

3.0 TECHNICAL EVALUATION

3.1 Licensee's Requested Change

The NRC staff issued Amendment No. 197 to Renewed Facility Operating License No. NPF-42 by letter dated July 27, 2011. This amendment approved the CSP and associated implementation schedule, and added a license condition requiring the licensee to fully implement and maintain the Commission-approved CSP. The implementation schedule was based on a template prepared by the Nuclear Energy Institute (NEI), which was transmitted to the NRC by letter dated February 28, 2011 (ADAMS Accession No. ML110600206). By letter dated March 1, 2011 (ADAMS Accession No. ML110070348), the NRC staff found the NEI template acceptable for licensees to use to develop their CSP implementation schedules. The licensee's proposed implementation schedule for the Cyber Security Program identified completion dates and bases for the following eight milestones:

1) Establish the Cyber Security Assessment Team (CSAT);

2) Identify Critical Systems (CSs) and Critical Digital Assets (CDAs);

3) Install deterministic one-way devices between lower level devices and higher level devices;

4) Implement the security control "Access Control For Portable And Mobile Devices";

5) Implement observation and identification of obvious cyber related tampering to existing insider mitigation rounds by incorporating the appropriate elements;

6) Identify, document, and implement technical cyber security controls in accordance with "Mitigation of Vulnerabilities and Application of Cyber Security Controls," for CDAs that could adversely impact the design function of physical security target set equipment;

7) Ongoing monitoring and assessment activities for those target set CDAs whose security controls have been implemented; and

8) Fully implement the CSP.

Currently, Milestone 8 of the WCGS CSP requires the licensee to fully implement the CSP by June 30, 2017. By letter dated June 14, 2016, the licensee proposed to modify the Milestone 8 completion date to December 31, 2017.

The licensee provided the following information pertinent to each of the criteria identified in the NRC guidance memorandum dated October 24, 2013.

1. Identification of the specific requirement or requirements of the cyber security plan that the licensee needs additional time to implement.

The licensee stated that CSP Section 3, "Analyzing Digital Computer Systems and Networks" and CSP Section 4, "Establishing, Implementing, and Maintaining the Cyber Security Program," need additional time to implement. It further noted that these sections describe requirements for application and maintenance of cyber security controls and described the process of addressing security controls. The licensee described specific requirements needing additional time including determining the need and implementation for automated security information and event management systems and designing/implementing these systems for monitoring activity on networks of CDAs, additional physical controls for CDAs outside the security protected area, and significant programmatic change management associated with approximately 50 procedure changes.

2. Detailed justification that describes the reason the licensee requires additional time to implement the specific requirement or requirements identified.

In its letter dated June 14, 2016, the licensee stated, in part;

> 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.

Also, the licensee stated that development of an endorsed written standard for interpreting and applying cyber security controls has continued to be a work-in-progress. The release of Revision 3 of NEI 13-10, "Cyber Security Control Assessments" 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. Defining the cyber security controls is resource intensive and without guidance for what "good" looks like for each control there is high risk of rework as industry interpretations change. The licensee further stated that CDA mitigation activities defined in Section 3.1.6 of the CSP, "Mitigation of Vulnerabilities and Application of Cyber Security Controls," are resource intensive, remediation activities need to be carefully considered, there are change management challenges, and the need for training on new programs, processes and procedures requires additional time to implement requirements of the CSP.

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

In its letter dated June 14, 2016, the licensee stated;

> 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 the licensee's overall cyber security program in the context of milestones already completed.

In its letter dated June 14, 2016, the licensee stated, in part;

> 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[1]) required actions by October 29, 2013. The completed activities provide a high degree of protection against cyber attacks while WCNOC implements the full program.

Further WCNOC has transitioned from the previous cyber security program. 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 discussion of the licensee's methodology for prioritizing completion of work for critical digital assets associated with significant safety, security, or emergency preparedness (SSEP) consequences and with reactivity effects in the balance of plant.

---

[1] NRC Memorandum from B. Westreich NRC to T. Blount NRC, "Enhanced Guidance for Licensee Near-Term Corrective Actions to Address Cyber Security Inspection Findings and Licensee Eligibility for "Good-Faith" Attempt Discretion," dated July 1, 2013 (security-related information, not publicly available).

In its letter dated June 14, 2016, the licensee stated, in part;

> 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 Determination Process. Prioritization for CDA assessments 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.

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

In its letter dated June 14, 2016, the licensee stated;

> A Quality Assurance (QA) surveillance of interim Implementation Milestones 1 through 7 has concluded that WCNOC has an effective program an[d] 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[2] 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 the licensee's CAP.

In its letter dated June 14, 2016, the licensee stated;

> 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.

---

[2] NRC Memorandum from B. Westreich NRC to T. Blount NRC, "Enhanced Guidance for Licensee Near-Term Corrective Actions to Address Cyber Security Inspection Findings and Licensee Eligibility for "Good-Faith" Attempt Discretion," dated July 1, 2013 (security-related information, not publicly available).

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

The licensee listed and discussed completed modifications and listed systems pending modifications. These are consistent with the discussion above and the CSP.

3.2 NRC Staff Evaluation

The NRC staff has evaluated the licensee's application using the regulatory requirements and guidance above. The NRC staff's evaluation is below. The staff finds that the actions necessary for full compliance with the WCGS CSP are reasonable as discussed below.

The licensee indicated that the activities associated with the CSP, as described in Milestones 1 through 7, were completed prior to December 31, 2012, and provide a high degree of protection against cyber attacks while WCNOC implements the full program. The NRC staff thus concludes that the activities already undertaken and completed by the licensee result in an increase to site security because the activities the licensee completed mitigate the most significant cyber attack vectors for the most significant CDAs. Therefore, the NRC has reasonable assurance that full implementation of the CSP by December 31, 2017, will provide adequate protection of the public health and safety and the common defense and security.

The licensee has stated that preparation for, and support of, NRC inspections, has required a significant commitment of time from WCNOCs most knowledgeable cyber security subject matter experts. This has drawn those subject matter experts and associated resources away from Milestone 8 implementation activities. Also development of an endorsed written standard for interpreting and applying cyber security controls has continued to be a work-in-progress. The release of Revision 3 of NEI 13-10 and then subsequently, Revision 4, appears to provide some reduction in level of effort needed to identify and apply those controls, but more time is needed to take full advantage of the guidance. Finally, the licensee stated that defining the cyber security controls is resource intensive, and because industry interpretations are subject to change and without guidance for what "good" looks like for each control, there is a high risk of rework. The licensee also noted the following:

- the CDA mitigation activities defined in Section 3.1.6 of the Cyber Security Plan are resource intensive.
- remediation activities need to be carefully considered.
- there are challenges associated with management changes, and
- training on new programs, processes and procedures may be required.

The NRC staff concludes that the licensee's request for additional time to implement Milestone 8 is reasonable given the unanticipated complexity, volume, and scope of the remaining work required to fully implement its CSP.

The licensee proposed a Milestone 8 completion date of December 31, 2017. The licensee stated that changing the completion date of Milestone 8 allows for sufficient time 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. The licensee stated the methodology for prioritizing Milestone 8 activities is centered on considerations for SSEP and BOP (continuity of power) consequences. The methodology is based on defense-in-depth, installed

configuration of the CDA, and susceptibility to commonly identified threat vectors. Prioritization of CDA assessments begins with safety related CDAs and continues through the lower priority non-safety and EP CDAs as follows: safety related CDAs, physical security CDAs, important to safety CDAs (including BOP CDAs that directly impact continuity of power) and control system CDAs, and non-safety related CDAs and SSEP CDAs. The NRC staff concludes that based on the tasks described above and the limited resources with the appropriate expertise to perform these activities, the licensee's methodology for prioritizing work on CDAs is appropriate. The staff further concludes that the licensee's request to delay final implementation of the CSP until December 31, 2017 is reasonable given the complexity of the remaining unanticipated work.

3.3 Technical Evaluation Conclusion

The NRC staff concludes that the licensee's request to delay full implementation of its CSP until December 31, 2017, is reasonable for the following reasons: (i) the licensee's implementation of Milestones 1 through 7 provides mitigation for significant cyber attack vectors for the most significant CDAs as discussed in the staff evaluation above; (ii) the scope of the work required to come into full compliance with the CSP implementation schedule was much more complicated than anticipated and not reasonably foreseeable when the CSP implementation schedule was originally developed; and (iii) the licensee has reasonably prioritized and scheduled the work required to come into full compliance with its CSP implementation schedule. Therefore, the staff finds the proposed change acceptable.

3.4 Revision to License Condition Paragraph 2.E

By letter dated June 14, 2016, the licensee proposed to modify paragraph 2.E of Renewed Facility Operating License No. NPF-42 for WCGS, which provides a license condition to require the licensees to fully implement and maintain in effect all provisions of the NRC-approved CSP.

The current license condition in paragraph 2.E of the Renewed Facility Operating License No. NPF-42 for WCGS states, in part;

> 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.

The revised portion of the license condition in paragraph 2.E of the Renewed Facility Operating License No. NPF-42 for WCGS would state:

> 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. 217.

4.0 REGULATORY COMMITMENTS

By letter dated June 14, 2016, the licensee made the following regulatory commitment:

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

The above stated commitment is consistent with the revised Milestone 8 implementation date proposed by the licensee and evaluated by the NRC staff.

5.0 STATE CONSULTATION

In accordance with the Commission's regulations, the Kansas State official was notified of the proposed issuance of the amendment on January 23, 2017. The State official had no comments.

5.0 ENVIRONMENTAL CONSIDERATION

This is an amendment to a 10 CFR Part 50 license that relates solely to safeguards matters and does not involve any significant construction impacts. This amendment is an administrative change to extend the date by which the licensee must have its cyber security plan fully implemented. Accordingly, the amendment meets the eligibility criteria for categorical exclusion set forth in 10 CFR 51.22(c)(12). Pursuant to 10 CFR 51.22(b), no environmental impact statement or environmental assessment need be prepared in connection with the issuance of the amendment.

6.0 CONCLUSION

The Commission has concluded, based on the considerations discussed above, that: (1) there is reasonable assurance that the health and safety of the public will not be endangered by operation in the proposed manner, (2) there is reasonable assurance that 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.

Principal Contributor: John Rycyna, NSIR/CSD

Date: March 24, 2017