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

March 16, 2017

Mr. Joseph W. Shea
Vice President, Nuclear Licensing
Tennessee Valley Authority
1101 Market Street, LP 3R-C
Chattanooga, TN 37402-2801

SUBJECT: WATTS BAR NUCLEAR PLANT, UNIT 2 – ISSUANCE OF AMENDMENT REGARDING CYBER SECURITY PLAN MILESTONE 8 IMPLEMENTATION SCHEDULE (CAC NO. MF8846)

Dear Mr. Shea:

The U.S. Nuclear Regulatory Commission has issued the enclosed Amendment No. 7 to Facility Operating License No. NPF-96 for the Watts Bar Nuclear Plant, Unit 2. This amendment consists of changes to the license in response to your application dated November 14, 2016.

This amendment revises the Cyber Security Plan (CSP) Milestone 8 full implementation date from March 31, 2017, to December 31, 2017, as set forth in the CSP Implementation Schedule; and revises paragraph 2.C.(7) in the Facility Operating License.

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

If you have any questions regarding this letter, please contact me at (301) 415-6020 or Robert.Schaaf@nrc.gov.

Sincerely,

Robert G. Schaaf, Senior Project Manager
Plant Licensing Branch II-2
Division of Operating Reactor Licensing
Office of Nuclear Reactor Regulation

Docket No. 50-391

Enclosures:
1. Amendment No. 7 to NPF-96
2. Safety Evaluation

cc w/enclosures: Distribution via Listserv

SUBJECT: WATTS BAR NUCLEAR PLANT, UNIT 2 – ISSUANCE OF AMENDMENT REGARDING CYBER SECURITY PLAN MILESTONE 8 IMPLEMENTATION SCHEDULE (CAC NO. MF8846) DATED MARCH 16, 2017

DISTRIBUTION:

PUBLIC
LPL2-2 R/F
RidsNrrDorlLpl2-2 Resource
RidsNrrLABClayton Resource
RidsRgn2MailCenter Resource
RidsNrrPMWattsBar Resource
RidsACRS_MailCTR Resource
RidsNsirCsd Resource
JRycyna, NSIR/CSD
MWentzel, NRR

ADAMS Accession No.: ML17033A333 *via e*mail

OFFICE	NRR/DORL/LPL2-2/PM	NRR/DORL/LPL2-2/LA	NSIR/CSD*
NAME	MWentzel	BClayton (PBlechman for)	JBeardsley
DATE	02/16/17	02/15/17	01/24/17
OFFICE	OGC / NLO	NRR/DORL/LPL2-2/BC	NRR/DORL/LPL2-2/PM
NAME	NSt. Amour	BBeasley (AHon for)	RSchaaf
DATE	03/15/17	03/16/17	03/16/17

OFFICIAL RECORD COPY

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

TENNESSEE VALLEY AUTHORITY

DOCKET NO. 50-391

WATTS BAR NUCLEAR PLANT, UNIT 2

AMENDMENT TO FACILITY OPERATING LICENSE

Amendment No. 7
License No. NPF-96

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

   A. The application for amendment by the Tennessee Valley Authority (TVA or the licensee) dated November 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, 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 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 paragraphs 2.C.(2) and 2.C.(7) of Facility Operating License No. NPF-96 are hereby amended to read as follows:

(2) Technical Specifications and Environmental Protection Plan

The Technical Specifications contained in Appendix A as revised through Amendment No. 7 and the Environmental Protection Plan contained in Appendix B, both of which are attached hereto, are hereby incorporated into this license. TVA shall operate the facility in accordance with the Technical Specifications and the Environmental Protection Plan.

(7) TVA 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 TVA approved CSP was discussed in NUREG-0847, Supplement 28, as amended by changes approved by License Amendment No. 7.

3. This license amendment is effective as of the date of its issuance, and shall be implemented within 30 days of issuance. The full implementation of the CSP shall be in accordance with the implementation schedule submitted by the licensee on November 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

Benjamin G. Beasley, Chief
Plant Licensing Branch II-2
Division of Operating Reactor Licensing
Office of Nuclear Reactor Regulation

Attachment:
Changes to the Facility
Operating License

Date of Issuance: March 16, 2017

ATTACHMENT TO LICENSE AMENDMENT NO. 7

WATTS BAR NUCLEAR PLANT, UNIT 2

FACILITY OPERATING LICENSE NO. NPF-96

DOCKET NO. 50-391

Replace the following page of Facility Operating License No. NPF-96 with the attached revised page. The revised page is identified by amendment number and contains marginal lines indicating the area of changes.

Facility Operating License

REMOVE	INSERT
3	3

C. The license shall be deemed to contain and is subject to the conditions specified in the Commission's regulations set forth in 10 CFR Chapter I and is subject to all applicable provisions of the Act, and to the rules, regulations, and orders of the Commission now or hereafter in effect, and is subject to the additional conditions specified or incorporated below.

(3) Maximum Power Level

TVA is authorized to operate the facility at reactor core power levels not in excess of 3411 megawatts thermal.

(4) Technical Specifications and Environmental Protection Plan

The Technical Specifications contained in Appendix A as revised through Amendment No. 7 and the Environmental Protection Plan contained in Appendix B, both of which are attached hereto, are hereby incorporated into this license. TVA shall operate the facility in accordance with the Technical Specifications and the Environmental Protection Plan.

(5) TVA shall implement permanent modifications to prevent overtopping of the embankments of the Fort Loudon Dam due to the Probable Maximum Flood by June 30, 2018.

(4) PAD4TCD may be used to establish core operating limits for Cycles 1 and 2 only. PAD4TCD may not be used to establish core operating limits for subsequent reload cycles.

(5) By December 31, 2017, the licensee shall report to the NRC that the actions to resolve the issues identified in Bulletin 2012-01, "Design Vulnerability in Electrical Power System," have been implemented.

(6) The licensee shall maintain in effect the provisions of the physical security plan, security personnel training and qualification plan, and safeguards contingency plan, and all amendments made pursuant to the authority of 10 CFR 50.90 and 50.54(p).

(7) TVA 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 TVA approved CSP was discussed in NUREG-0847, Supplement 28, as amended by changes approved by License Amendment No. 7.

(8) TVA shall implement and maintain in effect all provisions of the approved fire protection program as described in the Fire Protection Report for the facility, as described in NUREG-0847, Supplement 29, subject to the following provision:

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

SAFETY EVALUATION BY THE OFFICE OF NUCLEAR REACTOR REGULATION

RELATED TO AMENDMENT NO. 7 TO FACILITY OPERATING LICENSE NO. NPF-96

TENNESSEE VALLEY AUTHORITY

WATTS BAR NUCLEAR PLANT, UNIT 2

DOCKET NO. 50-391

1.0 INTRODUCTION

By letter dated November 14, 2016 (Agencywide Documents Access and Management System (ADAMS) Accession No. ML16320A161), Tennessee Valley Authority (TVA, the licensee) requested a change to the facility operating license for the Watts Bar Nuclear Plant (WBN), Unit 2.

The U.S. Nuclear Regulatory Commission (NRC or the Commission) staff initially reviewed and approved the licensee's Cyber Security Plan (CSP) implementation schedule in NUREG–0847, "Safety Evaluation Report Related to the Operation of Watts Bar Nuclear Plant, Unit 2, Docket Number 50-391," Supplement 24, dated September 2011 (ADAMS Accession No. ML11277A148). Subsequently, the NRC staff reviewed and approved NUREG–0847, Supplement 28, dated August 2015 (ADAMS Accession No. ML15229A195), which extended the CSP implementation schedule. This schedule required WBN Unit 2 to fully implement and maintain all provisions of the CSP no later than March 31, 2017.

The proposed change would revise the date of CSP Implementation Schedule Milestone 8 from March 31, 2017, to December 31, 2017; and would revise paragraph 2.C.(7) in the facility operating license. Milestone 8 of the CSP implementation schedule concerns the full implementation of the CSP. Portions of the letter dated November 14, 2016, contain sensitive unclassified non-safeguards (security- related) information and, accordingly, those portions are withheld from public disclosure. The NRC issued a proposed finding that the amendment involves no significant hazards consideration, published in the *Federal Register* on January 5, 2017 (82 FR 1370). The NRC has not received public comment on this determination.

2.0 REGULATORY EVALUATION

The NRC staff reviewed and approved the licensee's existing CSP implementation schedule in NUREG–0847, Supplement 28. The NRC staff considered the following regulatory requirements and guidance in its review of the current license amendment request 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 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.

- NRC 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), in which the NRC staff lists criteria that it would consider during its evaluations of 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, which 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, construction permit, or early site permit."

3.0 TECHNICAL EVALUATION

3.1 Licensee's Requested Change

The NRC staff approved the licensee's CSP implementation schedule, as discussed in NUREG–0847, Supplement 24, dated September 2011. The NRC staff approved a subsequent change to the CSP implementation schedule, as documented in NUREG–0847, Supplement 28, dated August 2015. 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 WBN Unit 2 CSP requires TVA to fully implement the CSP by March 31, 2017. In its November 14, 2016, application, TVA proposed to change the Milestone 8 completion date to December 31, 2017.

The licensee provided the following information pertinent to each of the eight 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 WBN Unit 2 has completed many of the actions required to address Milestone 8, "Full implementation of Watts Bar Nuclear Plant Cyber Security Plan for all SSEP [safety, security, and emergency preparedness] functions for WBN Unit 2 will be achieved." Additional time is required to assess, methodically plan, schedule and complete, and remediation actions for full compliance with the WBN Unit 2 CSP in addition to those associated with industry generic issues and possible lessons learned from ongoing Milestone 8 industry workshops.

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

The licensee stated that the proposed change would allow for the alignment of programmatic implementations for WBN Units 1 and 2 as a single site. This will allow WBN to coordinate implementation of program elements that will be shared between the two units. This is consistent with TVA's Browns Ferry Nuclear Plant and Sequoyah Nuclear Plant, which have a

single Milestone 8 completion date for each site. Additionally, during the performance of NRC Milestone 1 through 7 cyber security inspections, a number of issues were identified that were generic in nature. The NEI Cyber Security Task Force is working with the NRC staff to develop additional guidance for resolution of these generic issues. Additional interactions are already ongoing and resolution paths have been determined. While the currently available guidance documents and lessons learned from the NRC Milestone 1 through 7 inspection provide detailed insights into many aspects of a fully compliant cyber security program, there are additional implementation areas that NEI and NRC staff have determined need additional discussion. Focused workshops are in progress to review five specific programmatic areas, and to develop additional guidance based on those reviews. The timing for issuance of these additional clarifying guidance documents, referenced above in regard to the current Milestone 8 implementation date, does not allow for sufficient time to adequately plan, schedule, and implement remediation actions. Furthermore, in a letter dated December 21, 2015 (ADAMS Accession No. ML15351A065), the NRC staff endorsed Revision 4 to NEI 13-10, "Cyber Security Control Assessments." This revision provides clarification and examples for addressing the required security controls in Appendix D and certain security controls provided in Appendix E of NEI 08-09, "Cyber Security Plan for Nuclear Power Reactors," Revision 6 (ADAMS Accession No. ML101180437). Based on the recent endorsement, incorporation of this guidance into existing TVA processes and existing control assessments will require additional resource allocation that is not supported by the current Milestone 8 implementation date.

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

The licensee proposed a Milestone 8 completion date of December 31, 2017. The licensee stated the revised Milestone 8 date will allow for sufficient time to assess, plan, schedule, and implement any plant or programmatic changes required, including those resulting from the resolution of Milestone 1 through 7 industry generic issues and the completion of planned Milestone 8 industry workshops.

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.

The licensee stated that the completion of the CSP activities described in Milestones 1 through 7, which were completed prior to the WBN Unit 2 initial fuel load, provide a high degree of protection to ensure that digital computer and communication systems and networks associated with SSEP systems are sufficiently protected against cyber attacks. The licensee described various activities completed with Milestones 1 through 7 and noted that several elements of Milestone 8 have been completed. The licensee said that based on the activities already completed the proposed extension does not adversely impact the overall effectiveness of the CSP. The additional time will allow WBN Unit 2 to develop and implement certain technical and programmatic aspects of the CSP, including those based on the recent or planned issuance of additional guidance documents.

5. A description of the licensee's methodology for prioritizing completion of work for critical digital assets associated with significant safety consequences and with reactivity effects in the balance of plant.

The licensee stated its methodology for prioritizing completion of cyber security activities associated with significant SSEP consequences and with reactivity effects in the balance-of-plant focused on completing Milestones 1 through 7 prior to WBN Unit 2 initial fuel load, and implementation of remediation actions for Milestone 8 during available unit outages, consistent with its outage planning and design change processes. Work that can be done with the unit online is implemented consistent with work management processes and available resources. Prioritization of work was performed per TVA's work scheduling processes and was based on safety significance, required availability of significant systems, and consideration for all aspects and elements of risk management.

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

The licensee stated implementation of the requirements of Milestones 1 through 7 have been completed and provides a high degree of protection against cyber security-related attacks, during full program implementation. Cyber security assessments for all WBN Unit 2 CDAs have been completed and remediation actions have been determined for deficient controls. Many of the controls, which do not require a design change, have already been implemented. A Quality Assurance (QA) audit was completed in June 2016 for TVA Nuclear cyber security that found no significant deficiencies. TVA completed its most recent self-assessment of the WBN Unit 2 cyber security program in February 2015 with no significant deficiencies noted. Issues to address program improvements, which were identified during the audit and assessment activities, have been entered into the TVA Corrective Action Program (CAP). Quality Assurance audits will continue to monitor the performance of the cyber security program per the current QA biennial audit schedule. The NRC staff performed a Milestone 1 through 7 inspection of WBN in July 2014 and April 2015. All performance deficiencies were determined to be of very low safety significance. These deficiencies have been entered into the TVA CAP. Performance deficiencies and Unresolved Items noted that were determined to be generic in nature throughout the industry, are being addressed. These actions show evidence of strong cyber security program performance up to the submittal of this license amendment request.

7. A discussion of cyber security issues pending in the licensee's CAP.

The TVA CAP is used to document cyber security issues in order to trend, correct, implement, and improve the cyber security program for WBN. The CAP documents and tracks cyber security-required actions, including remediation actions identified during cyber security assessments of CDAs and issues identified during ongoing program surveillances and assessments. Adverse trends are monitored for program improvement and are tracked via the CAP. The licensee listed actions pending in the CAP. They are consistent with the information provided in other sections of the license amendment request.

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

The licensee stated physical modifications for approximately 98-percent of the defensive model have been installed. Additional configuration and setup are still required for these devices. Any additional modifications or programmatic changes required, based on the issuance of guidance for industry generic issues or the Milestone 8 workshops, will be entered into the TVA CAP for resolution prior to the requested Milestone 8 completion date. Completed modifications were listed.

3.2 NRC Staff Evaluation

The NRC staff has evaluated the licensee's application using the regulatory requirements and the guidance set forth above. The NRC staff's evaluation is below.

The licensee stated that additional time is required to assess, methodically plan, schedule, and complete remediation actions for full compliance with the WBN Unit 2 CSP, in addition to those associated with industry generic issues and possible lessons learned from ongoing Milestone 8 industry workshops.

The licensee indicated completion of activities associated with the CSP, as described in Milestones 1 through 7 and completed prior to December 31, 2012, provides a high degree of protection to ensure that digital computer and communication systems and networks associated with SSEPs are sufficiently protected against cyber attacks. The licensee said that based on the activities already completed, the proposed extension does not adversely impact the overall effectiveness of the CSP. The additional time will allow WBN Unit 2 to develop and implement certain technical and programmatic aspects of the CSP, including those based on the recent or planned issuance of additional guidance documents. The NRC staff finds that the licensee's site is much more secure after implementation of Milestones 1 through 7 because the activities the licensee completed mitigate the most significant cyber attack vectors for the most significant CDAs.

The licensee said that during the performance of NRC Milestone 1 through 7 cyber security inspections, a number of issues were identified that were generic in nature. Resolution paths have been determined. The current Milestone 8 implementation date does not allow for sufficient time to adequately plan, schedule, and implement remediation actions. The requested date bounds the completion of all individual asset security control design remediation actions. The NRC staff has had extensive interaction with the nuclear industry since licensees first developed their CSP implementation schedules. Based on this interaction, the NRC staff recognizes that CDA security control design remediation actions are much more complex and resource intensive than originally anticipated and that the licensee has a large number of additional tasks not originally considered when developing its current CSP implementation schedule. Accordingly, the NRC staff finds that the licensee's request for additional time to implement Milestone 8 is reasonable, given the unanticipated complexity and scope of the work required to come into full compliance with 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 will allow for sufficient time to assess, plan, schedule, and implement any plant or programmatic changes required resulting from the resolution of Milestone 1 through 7 industry generic issues and the completion of planned industry workshops for Milestone 8. The licensee stated its methodology for prioritizing completion of cyber security activities associated with significant SSEP consequences and with reactivity effects in the balance-of-plant focused on competing Milestones 1 through 7 by initial fuel load and implementation of remediation actions for Milestone 8 during the available refueling outages consistent with TVA outage planning and design change processes. Work that can be done with the units online is implemented consistent with work management processes and available resources. Prioritization of work is performed per TVA's work scheduling processes and is based on safety significance, required availability of significant systems, and consideration for all aspects and elements of risk management. The NRC staff finds that based on the description of work 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 NRC staff further finds that the licensees 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; and (iii) the licensee has reasonably prioritized and scheduled the work required to come into full compliance with its CSP implementation schedule. The NRC staff also concludes that, upon full implementation of the licensee's cyber security program, the requirements of the licensee's CSP and 10 CFR 73.54 will be met. Therefore, the NRC staff finds the proposed change acceptable.

3.4 Revision to License Condition 2.C.(7)

By letter dated November 14, 2016, the licensee proposed to modify paragraph 2.C.(7) of Facility Operating License No. NPF-96, which provides a license condition to require the licensee to fully implement and maintain in effect all provisions of the NRC-approved CSP. The current paragraph 2.C.(7) of Facility Operating License No. NPF-96 for WBN Unit 2 states:

> TVA 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 TVA approved CSP was discussed in NUREG-0847, Supplement 28.

The revised license condition in paragraph 2.C.(7) of Facility Operating License No. NPF-96 for WBN Unit 2 would state:

> TVA 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 TVA approved CSP was discussed in NUREG-0847, Supplement 28, as amended by changes approved by License Amendment No. 7.

Based on the information in Section 3.0 of this safety evaluation and the modified license condition described above, the NRC staff concludes this is acceptable.

4.0 STATE CONSULTATION

In accordance with the Commission's regulations, the Tennessee State official was notified of the proposed issuance of the amendment on February 16, 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

Date: March 16, 2017