



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

June 23, 2016

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 1 – ISSUANCE OF AMENDMENT
REGARDING CYBER SECURITY PLAN MILESTONE 8 IMPLEMENTATION
SCHEDULE (CAC NO. MF7429)

Dear Mr. Shea:

The U.S. Nuclear Regulatory Commission has issued the enclosed Amendment No. 106 to Facility Operating License No. NPF-90 for the Watts Bar Nuclear Plant, Unit 1. This amendment consists of changes to the license in response to your application dated March 4, 2016.

The amendment revises the Cyber Security Plan (CSP) Milestone 8 full implementation date from June 30, 2016, to December 31, 2017, as set forth in the CSP Implementation Schedule; and revises Paragraph 2.E(2) 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.

Sincerely,

A handwritten signature in black ink, appearing to read "Robert G. Schaaf".

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

Docket No. 50-390

Enclosures:

1. Amendment No. 106 to NPF-90
2. Safety Evaluation

cc w/encls: Distribution via Listserv



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

TENNESSEE VALLEY AUTHORITY

DOCKET NO. 50-390

WATTS BAR NUCLEAR PLANT, UNIT 1

AMENDMENT TO FACILITY OPERATING LICENSE

Amendment No. 106
License No. NPF-90

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 march 4, 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 Title 10 of the *Code of Federal Regulations* (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 Facility Operating License No. NPF-90 is amended by changes to paragraphs 2.C(2) and 2.E(2), as indicated in the attachment to this license amendment.
3. This license amendment is effective as of the date of its issuance, and shall be implemented within 14 days of issuance.

FOR THE NUCLEAR REGULATORY COMMISSION

A handwritten signature in black ink, appearing to read "Tracy Orf". The signature is fluid and cursive, with a large initial "T" and a long, sweeping underline.

Tracy Orf, Acting Chief
Plant Licensing Branch II-2
Division of Operating Reactor Licensing
Office of Nuclear Reactor Regulation

Attachment:
Changes to the Operating License

Date of Issuance: June 23, 2016

ATTACHMENT TO LICENSE AMENDMENT NO. 106

FACILITY OPERATING LICENSE NO. NPF-90

DOCKET NO. 50-390

Replace the following page of Facility Operating License NPF-90 with the attached revised pages. The revised pages are identified by amendment number and contains a marginal line indicating the area of change.

Facility Operating License

REMOVE

3

5

INSERT

3

5

- (4) TVA, pursuant to the Act and 10 CFR Parts 30, 40 and 70, to receive, possess, and use in amounts as required, any byproduct, source or special nuclear material without restriction to chemical or physical form, for sample analysis, instrument calibration, or other activity associated with radioactive apparatus or components; and
 - (5) TVA, pursuant to the Act and 10 CFR Parts 30, 40 and 70, to possess, but not separate, such byproduct and special nuclear materials as may be produced by the operation of the facility.
- C. This 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.
- (1) Maximum Power Level
TVA is authorized to operate the facility at reactor core power levels not in excess of 3459 megawatts thermal.
 - (2) Technical Specifications and Environmental Protection Plan
The Technical Specifications contained in Appendix A as revised through Amendment No. 106 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.
 - (3) Safety Parameter Display System (SPDS) (Section 18.2 of SER Supplements 5 and 15)
Prior to startup following the first refueling outage, TVA shall accomplish the necessary activities, provide acceptable responses, and implement all proposed corrective actions related to having the Watts Bar Unit 1 SPDS operational.
 - (4) Vehicle Bomb Control Program (Section 13.6.9 of SSER 20)
During the period of the exemption granted in paragraph 2.D.(3) of this license, in implementing the power ascension phase of the approved initial test program, TVA shall not exceed 50% power until the requirements of 10 CFR 73.55(c)(7) and (8) are fully implemented. TVA shall submit a letter under oath or affirmation when the requirements of 73.55(c)(7) and (8) have been fully implemented.

- (2) The facility was previously granted an exemption from the criticality monitoring requirements of 10 CFR 70.24 (see Special Nuclear Material License No. SNM-1861 dated September 5, 1979). The technical justification is contained in Section 9.1 of Supplement 5 to the Safety Evaluation Report, and the staff's environmental assessment was published on April 18, 1985 (50 FR 15516). The facility is hereby exempted from the criticality alarm system provisions of 10 CFR 70.24 so far as this section applies to the storage of fuel assemblies held under this license.
 - (3) The facility requires an exemption from 10 CFR 73.55(c)(10). The justification for this exemption is contained in Section 13.6.9 of Supplement 15 and 20 to the Safety Evaluation Report. The staff's environmental assessment was published on April 25, 1995 (60 FR 20291). Pursuant to 10 CFR 73.5, the facility is exempted from the stated implementation schedule of the surface vehicle bomb rule, and may implement the same as late as February 17, 1996.
 - (4) The facility was previously granted an exemption from certain requirements of 10 CFR 73.55(d)(5) relating to the returning of picture badges upon exit from the protected areas, such that individuals not employed by TVA who are authorized unescorted access into protected areas can take their badges offsite (see 59 FR 66061, December 22, 1994). The granting of this exemption is hereby affirmed.
 - (5) The facility was previously granted an exemption from certain requirements of 10 CFR 50, Appendix E, such that the State of Tennessee, which is within the ingestion exposure pathway emergency planning zone, need not participate in the November 1995 full-participation exercise (see 60 FR 54526, October 24, 1995). The granting of this exemption is hereby affirmed.
- E.
- (1) TVA 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 50.54(p). The combined set of plans, which contains Safeguards Information protected under 10 CFR 73.21, is entitled: "Watts Bar Nuclear Plant Security Plan, Training and Qualification Plan, and Safeguards Contingency Plan, Revision 3," submitted by letter dated May 16, 2006.
 - (2) 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 CSP was approved by License Amendment No. 87, as amended by changes approved by License Amendment Nos. 97, 101, and 106.



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

SAFETY EVALUATION BY THE OFFICE OF NUCLEAR REACTOR REGULATION
RELATED TO AMENDMENT NO. 106 TO FACILITY OPERATING LICENSE NO. NPF-90
TENNESSEE VALLEY AUTHORITY
WATTS BAR NUCLEAR PLANT, UNIT 1
DOCKET NO. 50-390

1.0 INTRODUCTION

By letter dated March 4, 2016 (Agencywide Documents Access and Management System (ADAMS) Accession No. ML16064A488), Tennessee Valley Authority (TVA, the licensee) requested a change to the facility operating license for the Watts Bar Nuclear Plant (WBN) Unit 1.

The U.S. Nuclear Regulatory Commission (NRC or the Commission) staff initially reviewed and approved the licensee's Cyber Security Plan (CSP) implementation schedule by WBN Unit 1 License Amendment No. 87 dated August 30, 2011 (ADAMS Accession No. ML11200A229). Subsequently, NRC staff reviewed and approved Amendment No. 97, dated September 29, 2014, which extended the CSP implementation schedule (ADAMS Accession No. ML14255A152). This schedule required WBN Unit 1 to fully implement and maintain all provisions of the CSP no later than June 30, 2016. By letter dated August 7, 2015 (ADAMS Accession No. ML15177A334), the NRC staff approved Amendment No. 101, which clarified the demarcation point between assets under NRC jurisdiction, and those under the jurisdiction of the Federal Energy Regulatory Commission.

The proposed change would revise the date of CSP Implementation Schedule Milestone 8 from June 30, 2016, to December 31, 2017; and would revise Paragraph 2.E(2) in the facility operating license. Milestone 8 of the CSP implementation schedule and paragraph 2.E(2) concern the full implementation of the CSP. Portions of the letter dated March 4, 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 April 19, 2016 (81 FR 23012). The NRC has not received public comment on this determination.

2.0 REGULATORY EVALUATION

The NRC staff considered the following regulatory requirements and guidance in its review of the 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 to consider during 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, that states "[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 pursuant to 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 issued Amendment No. 87 to Facility Operating License NPF-90 for WBN Unit 1 by letter dated July 28, 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, the NRC staff found the NEI template acceptable for licensees to use to develop their CSP implementation schedules (ADAMS Accession No. ML110070348).

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 1 CSP requires the licensee to fully implement the CSP by June 30, 2016. By letter dated March 4, 2016, the licensee proposed to modify the Milestone 8 completion date to December 15, 2017.

The licensee submitted its March 4, 2016, letter using the NRC staff's guidance to evaluate requests to postpone Milestone 8 implementation dates. The licensee's application addressed all the criteria in the guidance. The intent of the staggered cyber security implementation schedule was for licensees to demonstrate ongoing implementation of their cyber security program prior to full implementation, which was scheduled for the date specified in Milestone 8. The licensee completed seven other milestones (Milestone 1 through Milestone 7) by December 31, 2012. Activities included establishing a CSAT, identifying CSs and CDAs, installing deterministic one-way devices between defensive levels, implementing access control for portable and mobile devices, implementing methods to observe and identify obvious cyber related tampering, and conducting ongoing monitoring and assessment activities for target set CDAs. In their aggregate, the interim milestones demonstrate ongoing implementation of the cyber security program.

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 said that all actions required for full compliance with the WBN, Unit 1, CSP are scheduled to be completed prior to the current Milestone 8 implementation date with the exception of those associated with industry generic issues and possible lessons learned from planned Milestone 8 industry workshops. Implementation of these items will require additional time to assess, methodically plan, schedule, and complete remediation actions.

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

The licensee said that during the performance of NRC Milestones 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.

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

The licensee said that it is requesting an extension to the Milestone 8 completion date from June 30, 2016, to December 31, 2017. The revised Milestone 8 date will allow for sufficient time to assess, plan, schedule, and implement any plant or programmatic changes resulting from the resolution of Milestones 1 through 7 industry generic issues.

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 said that the completion of Milestones 1 through 7 prior to December 31, 2012, provides a high degree of protection to ensure that digital computer and communication systems and networks associated with safety, security, and emergency preparedness (SSEP) systems are sufficiently protected against cyber attacks. It then discussed implementation of each of the milestones and noted that several elements of Milestone 8 have already been implemented. Based on the activities already completed, and those planned to be completed by the current Milestone 8 implementation date, the licensee stated that the proposed extension does not adversely impact the overall effectiveness of the Cyber Security Program. The additional time will allow WBN to develop and implement certain technical and programmatic aspects of the Cyber Security Program.

5. A description of the licensee'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.

The licensee said that 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 December 31, 2012, and implementation of remediation actions for Milestone 8 during available refueling outages consistent with 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 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 said that implementation of the requirements of Milestones 1 through 7 has been completed and provides a high degree of protection against cyber attacks during full program implementation. Cyber security assessments for all WBN, Unit 1 CDAs have been completed and remediation actions have been determined for deficient controls. Many of the controls that do not require a design change have already been implemented. A Quality Assurance (QA) audit was completed in October 2014 for WBN cyber security that found no significant deficiencies. The most recent self-assessment of the cyber security program was completed 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 performed Milestones 1 through 7 inspections 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 were determined to be generic.

7. A discussion of cyber security issues pending in the licensee's corrective action program.

The licensee said that the TVA CAP is used to document cyber security issues in order to trend, correct, implement, and improve the cyber security program for WBN, Unit 1. 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. A list of items pending in the CAP was provided.

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

The licensee said that modifications to implement approximately 98-percent of the defensive model have been completed. Some modifications that have been implemented were listed. The licensee also said that the remaining known actions for Milestone 8 are scheduled to be completed prior to the current Milestone 8 completion date. Any additional modifications or programmatic changes required based on industry generic issues will be entered into the TVA CAP for resolution.

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 NRC staff finds that the actions the licensee noted as being required to implement CSP, Section 3, "Analyzing Digital Computer

Systems and Networks,” and Section 4, “Establishing, Implementing and Maintaining the Cyber Security Program,” 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 to ensure that the most significant digital computer and communication systems and networks associated with SSEP functions are sufficiently protected against cyber attacks. The NRC staff concludes that the licensee’s site is more secure after the implementation of Milestones 1 through 7 because the activities the licensee has 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 stated that the current Milestone 8 implementation date does not allow for sufficient time to adequately plan, schedule, and implement remediation actions. The NRC staff recognizes that CDA assessment work including application of controls and remediation is much more complex and resource intensive than originally anticipated. As a result, the licensee has a large number of additional tasks not originally considered when developing its CSP implementation schedule. 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 will allow for sufficient time to assess, plan, schedule, and implement any plant or programmatic changes resulting from the resolution of industry generic issues. 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 by December 31, 2012, and implementation of remediation actions for Milestone 8 during available refueling outages consistent with TVA’s outage planning and design change processes. The licensee also stated that work that can be done with the units 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. The NRC staff concludes that based on the large number of 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.

3.4 Revision to License Condition 2.E(2)

In its letter dated March 4, 2016, the licensee proposed to modify Paragraph 2.E(2) of Facility Operating License No. NPF-90 for WBN Unit 1, which provides a license condition to require the licensee to fully implement and maintain in effect all provisions of the Commission-approved CSP.

The current license condition in Paragraph 2.E(2) of Facility Operating License No. NPF-90 for WBN Unit 1 states:

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 CSP was approved by License Amendment No. 87, as amended by changes approved by License Amendment Nos. 97 and 101.

The revised license condition in Paragraph 2.E(2) of Facility Operating License No. NPF-90 for WBN Unit 1 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 CSP was approved by License Amendment No. 87, as amended by changes approved by License Amendment Nos. 97, 101, and 106.

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. 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.

Contributors: Liem Nguyen
John Rycyna

Date: June 23, 2016

June 23, 2016

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 1 – ISSUANCE OF AMENDMENT
REGARDING CYBER SECURITY PLAN MILESTONE 8 IMPLEMENTATION
SCHEDULE (CAC NO. MF7429)

Dear Mr. Shea:

The U.S. Nuclear Regulatory Commission has issued the enclosed Amendment No. 106 to Facility Operating License No. NPF-90 for the Watts Bar Nuclear Plant, Unit 1. This amendment consists of changes to the license in response to your application dated March 4, 2016.

The amendment revises the Cyber Security Plan (CSP) Milestone 8 full implementation date from June 30, 2016, to December 31, 2017, as set forth in the CSP Implementation Schedule; and revises Paragraph 2.E(2) 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.

Sincerely,

/RA/

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

Docket No. 50-390

Enclosures:

1. Amendment No. 106 to NPF-90
2. Safety Evaluation

cc w/encls: Distribution via Listserv

DISTRIBUTION:

PUBLIC	RidsNrrLABClaytonResource	JBeardsley, NSIR/CSD
LPL 2-2 R/F	RidsACRS_MailCTR Resource	JRycyna, NSIR/CSD
RidsNrrDorIDpr Resource	RidsRgn2MailCenter Resource	RecordsAmend
RidsNrrDorLpl2-2 Resource	RidsNrrPMWattsBar Resource	

ADAMS Accession No. ML16146A745

*** via e-mail dated April 15, 2016**

OFFICE	NRR/DORL/LPL2-2/PM	NRR/DORL/LPL2-2/LA	NSIR/CSD*	OGC
NAME	RSchaaf	BClayton	JBeardsley	JBielecki
DATE	6/22/2016	6/22/2016	4/15/2016	6/22/2016
OFFICE	NRR/DORL/LPL2-2/BC(A)	NRR/DORL/LPL2-2/PM		
NAME	TOrf	RSchaaf		
DATE	6/23/2016	6/23/2016		

OFFICIAL RECORD COPY