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

January 13, 2015

Mr. Oscar A. Limpias
Vice President-Nuclear and CNO
Nebraska Public Power District
72676 648A Avenue
Brownville, NE 68321

SUBJECT: COOPER NUCLEAR STATION – CORRECTIONS FOR AMENDMENT NO. 249 (TAC NO. MF3631)

Dear Mr. Limpias:

By letter dated December 12, 2014 (Agencywide Documents Access and Management System (ADAMS) Accession No. ML14323A644), the U.S. Nuclear Regulatory Commission (NRC) issued Amendment No. 249 to Renewed Facility Operating License No. DPR-46 for the Cooper Nuclear Station associated with the revised schedule for implementation of the Cyber Security Plan. This amendment was in response to your application dated March 14, 2014, as supplemented by letter dated July 28, 2014. It was discovered that there were some errors in the NRC staff's safety evaluation, however, these errors were minor and did not affect the NRC staff's overall conclusions associated with Amendment No. 249.

Enclosed is the revised safety evaluation to be included with the issued amendment, with revision bars indicating the areas of change. We regret any inconvenience this may have caused.

Sincerely,

Siva P. Lingam

Siva P. Lingam, Project Manager
Plant Licensing Branch IV-1
Division of Operating Reactor Licensing
Office of Nuclear Reactor Regulation

Docket No. 50-298

Enclosure:
Revised Safety Evaluation

cc w/encl: Distribution via Listserv

ENCLOSURE

REVISED SAFETY EVALUATION RELATED TO
AMENDMENT NO. 249 DATED DECEMBER 12, 2014

NEBRASKA PUBLIC POWER DISTRICT

COOPER NUCLEAR STATION

DOCKET NO. 50-298

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

SAFETY EVALUATION BY THE OFFICE OF NUCLEAR REACTOR REGULATION

RELATED TO AMENDMENT NO. 249 TO

RENEWED FACILITY OPERATING LICENSE NO. DPR-46

NEBRASKA PUBLIC POWER DISTRICT

COOPER NUCLEAR STATION

DOCKET NO. 50-298

1.0 INTRODUCTION

By application dated March 14, 2014 (Agencywide Documents Access and Management System (ADAMS) Accession No. ML14078A039) as supplemented by letter dated July 28, 2014 (ADAMS Accession No. ML14211A527), the Nebraska Public Power District (NPPD, the licensee) requested a change to the renewed facility operating license (FOL) for Cooper Nuclear Station (CNS). Portions of the letters dated March 14, 2014 and July 28, 2014, contain sensitive unclassified non-safeguards information and accordingly, those portions are withheld from public disclosure in accordance with the provisions of paragraph 2.390(d)(1) of Title 10 of the *Code of Federal Regulations* (10 CFR).

The supplemental letter dated July 28, 2014, provided additional information that clarified the application, did not expand the scope of the application as originally noticed, and did not change the U.S. Nuclear Regulatory Commission (NRC) staff's original proposed no significant hazards consideration determination as published in the *Federal Register* on July 8, 2014 (79 FR 38580).

The proposed change would revise the date of Cyber Security Plan (CSP) Implementation Schedule Milestone 8 and the existing license conditions in the renewed FOL. Milestone 8 of the CSP implementation schedule concerns the full implementation of the CSP.

2.0 REGULATORY EVALUATION

The NRC staff reviewed and approved the licensee's existing CSP implementation schedule by License Amendment No. 238 dated July 27, 2011 (ADAMS Accession No. ML111801081), to Renewed FOL No. DPR-46 for the CNS, concurrent with the incorporation of the CSP into the facility's current licensing basis. By letter dated March 14, 2014, as supplemented by letter dated July 28, 2014, the licensee requested to change Milestone 8 of the CSP implementation

schedule. 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:

- The regulations in 10 CFR 73.54, "Protection of digital computer and communication systems and networks," which state, in part, that "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 licenses includes a license condition that requires the licensee to fully implement and maintain in effect all provisions of the Commission-approved CSP (License Condition 2.C.(3) for the CNS Renewed FOL).

- 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 (publicly available at 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 "[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.

3.0 TECHNICAL EVALUATION

3.1 Background

The NRC staff issued Amendment No. 238 to Renewed FOL DPR-46 for CNS on July 27, 2011, approving the licensee's CSP. The NRC staff also approved the licensee's CSP implementation schedule, as discussed in the safety evaluation issued with Amendment No. 238. In addition, the NRC staff approved changes to the scope of CSP Milestone 6 on December 12, 2012, and issued Amendment No. 244 (ADAMS Accession No. ML12318A160) to reflect the approved schedule change for implementation of the operational and management controls for the CSP per Milestone 6 to coincide with the implementation of Milestone 8. As such, implementation of the operational and management controls associated with Milestone 6 will also be postponed to be coincident with the requested change in implementation of Milestone 8 per this amendment

request. The implementation schedule had been submitted by the licensee based on a template developed by the Nuclear Energy Institute (NEI) (ADAMS Accession No. ML110600206). 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:

- Establish the Cyber Security Assessment Team (CSAT);
- Identify Critical Systems (CSs) and Critical Digital Assets (CDAs);
- Install a deterministic one-way device between lower level devices and higher level devices;
- Implement the security control "Access Control For Portable And Mobile Devices";
- Implement observation and identification of obvious cyber related tampering to existing insider mitigation rounds;
- Identify, document, and implement 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;
- Commence ongoing monitoring and assessment activities for those target set CDAs whose security controls have been implemented; and
- Fully implement the CSP for all safety, security, and emergency preparedness functions.

3.2 Licensee's Proposed Change

Currently, Milestone 8 of the NPPD CSP requires the licensee to fully implement the CSP by December 15, 2014. By letter dated March 14, 2014, as supplemented by letter dated July 28, 2014, the licensee has proposed to change the Milestone 8 completion date to June 30, 2017. The licensee also proposed to modify Paragraph 2.C.(3) of Renewed FOL DPR-46 for CNS to reflect the revised full implementation schedule for the CSP. The proposed change also, in effect, changes the implementation of the operational and management controls associated with Milestone 6 to the revised Milestone 8 implementation date since Amendment No. 244 approved implementation of the operational and management controls to coincide with the implementation of Milestone 8.

3.3 NRC Staff Evaluation

The licensee's request dated March 14, 2014, as supplemented by letter dated July 28, 2014, is consistent with the NRC staff guidance memorandum dated October 24, 2013, developed to

evaluate requests to postpone Milestone 8 implementation dates. The intent of the cyber security implementation schedule was for licensees to demonstrate ongoing implementation of their cyber security program prior to full implementation, which is set for the date specified in Milestone 8. Activities include 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 criteria stated in the NRC guidance memorandum dated October 24, 2013, and addressed by the licensee as justification for its request are:

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

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

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

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.

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.

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

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

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

The NRC staff evaluated the licensee's request based on the above review criteria specified 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 identified specific CSP requirements requiring additional time to implement. The licensee also stated that there are specific tasks related to the requirements requiring additional time to implement. These tasks are related to aspects of NEI 08-09 Appendix D and Appendix E. The licensee provided a list of additional activities required to implement the CSP requirements.

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

Delays were encountered in finalizing the assessment process. The licensee also noted there are approximately 1,600 CDAs at CNS and there are hundreds of security control attributes resulting in a significant project involving plant components and systems, and substantial planning and resources. Additionally, changes to CDAs and procedures must be integrated into the plant operational schedule including on-line operations, maintenance and testing, as well as planning and execution of refueling outages. There is insufficient time to conduct modification planning activities, procurement, and pre-installation testing to allow inclusion of modifications in the fall 2014 refueling outage scope. Some plant modifications to control and data acquisition networks cannot be applied during power operations. The proposed implementation date change allows for an additional refueling outage to implement potential modifications. The licensee then provided detailed justification for additional time to fully implement the CSP.

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 June 30, 2017. The licensee also stated that changing the completion date of Milestone 8 will encompass one additional refueling outage and provide adequate time to plan and schedule the implementation of the modifications identified as the result of CDA assessments plus a contingency of approximately 6 months.

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 indicated the impact of the requested additional implementation time on the effectiveness of the overall cyber security program is considered to be very low, because the milestones already completed have resulted in a high degree of protection of safety-related, important-to-safety, and security CDAs against common threat vectors. With the exception of implementation of the operational and management controls associated with Milestone 6, CNS completed the implementation of Milestones 1 through 7 as required by December 31, 2012. Subsequently, in 2013, CNS completed additional actions to address issues identified for Milestone 4. Implementation of the operational and management controls associated with Milestone 6 was previously approved by the NRC in Amendment 244 to coincide with the implementation of Milestone 8. The licensee provided details about implementation of each completed milestone.

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 stated its methodology for prioritizing CDA activities is centered on considerations for safety, security, or emergency preparedness (SSEP), and balance-of-plant (continuity of power) consequences. Because CDAs are plant components, prioritization of work on CDAs follows the normal work management process. The licensee's Cyber Security organization will provide input to this process, taking into consideration defense-in-depth, installed (secure) configuration of the CDA, susceptibility to identified threat vectors, and availability of the assets. While CNS will attempt to address components with the highest risk first, work will depend on the availability of the assets. Some modifications will require the components to be taken out of service or may require a plant outage to perform. In addition, CNS will place a high priority on any emergent issue involving a CDA that could potentially challenge the established cyber security barriers.

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

The licensee stated that there has been no identified compromise of SSEP functions by cyber means at CNS. CSP Milestones 1 through 7 actions were successfully completed by December 31, 2012. Implementation of the operational and management controls associated with Milestone 6 was previously approved by the NRC in Amendment 244 to coincide with the implementation of Milestone 8. These actions provide a high degree of protection against cyber attacks while full program actions required to provide defense-in-depth are in progress. Performance deficiencies and recommendations to close program performance gaps are entered in CNS' corrective action program (CAP). A formal quality assurance audit was conducted in the first quarter of 2013 pursuant to the 24-month physical security program review required by 10 CFR 73.55(m), which included review of cyber security program implementation. The issues were entered into the CAP and have been resolved.

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

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 CNS CAP. It provided three examples of non-significant cyber security issues currently in the CAP.

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

The licensee provided a brief discussion of completed and pending modifications.

3.3 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 concludes that the actions the licensee noted as being required to implement the cyber security program based on the guidance in NEI 08-09 Appendix D and Appendix E are considered reasonable as discussed below.

With the exception of implementation of the operational and management controls associated with Milestone 6, the licensee indicated that completion of 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 protected against cyber attacks. Implementation of the operational and management controls associated with Milestone 6 was previously approved by the NRC in Amendment 244 to coincide with the implementation of Milestone 8. The licensee also stated that there has been no identified compromise of SSEP functions from cyber means.

The licensee indicated that completion of the activities associated with the CSP, as described in Milestones 1 through 5 and 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 protected against cyber attacks. A review was performed in 2012 that determined there were no CDAs that could adversely impact the design function of physical security target set equipment. In 2013, based upon the receipt of industry operating experience, an additional review of target sets for potential CDAs was conducted. The results of this review are being dispositioned in the CAP.

Milestone 6 was previously approved by the NRC in Amendment 244 to coincide with the implementation of Milestone 8. The interim milestones 1 through 5, and 7 provide sufficient cyber security protection during the interim period until the cyber security program is fully implemented. Many of the licensee's existing programs are primarily procedure-based programs and must be implemented in coordination with the comprehensive cyber security program. The existing programs currently in place at CNS (e.g., physical protection, maintenance, configuration management, and operating experience) provide sufficient operational and management cyber security protection during the interim period until the cyber security program is fully implemented. The NRC staff concludes that the licensee's site is more secure after the implementation of these cyber security controls, because the activities the licensee completed mitigate significant cyber attack vectors for significant CDAs. Therefore, the NRC staff has reasonable assurance that full implementation of the CSP by June 30, 2017 will provide adequate protection of the public health and safety and the common defense and security.

The licensee has stated that the scope of actions required to fully implement its CSP were not anticipated when the implementation schedule was originally determined. The NRC staff recognizes that CDA assessment work including application of controls is much more complex and resource intensive than originally anticipated, in part due to the NRC expanding the scope

of the cyber security requirements to include balance of plant. 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 and scope of the work required to come into full compliance with its CSP.

The licensee proposed a Milestone 8 completion date of June 30, 2017. The licensee stated that changing the completion date of Milestone 8 allows for an additional refueling outage to methodically plan, implement, and test the required additions or changes and allows those additions or changes that require a design change to be performed. The licensee stated its methodology for prioritizing Milestone 8 activities is centered on considerations for SSEP and balance-of-plant (continuity of power) consequences. The methodology is based on defense-in–depth, installed configuration of the CDA and susceptibility to the five commonly identified threat vectors. The NRC staff concludes that based on the large number of digital assets 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 concludes that the licensee's request to delay final implementation of the CSP until June 30, 2017, is reasonable given the complexity of the remaining unanticipated work and the need to perform certain work during the scheduled refueling outage.

3.4 Technical Evaluation Conclusion

The NRC staff concludes that the licensee's request to delay full implementation of its CSP until June 30, 2017 is reasonable for the following reasons: (i) the licensee's implementation of cyber security controls to date provides mitigation for significant cyber attack vectors for the most significant CDAs as discussed in the staff conclusion 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 scheduled 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.

3.5 Revision to License Condition 2.C.(3)

By letter dated March 14, 2014, as supplemented by letter dated July 28, 2014, the licensee proposed to modify Paragraph 2.C.(3) of Renewed FOL No. DPR-46, which provides a license condition to require the licensee to fully implement and maintain in effect all provisions of the NRC-approved CSP.

Current License Condition

The current license condition in Paragraph 2.C.(3) of Renewed FOL No. DPR-46 for CSN states, in part, that

> NPPD 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 NPPD

> CSP was approved by License Amendment No. 238 as supplemented by a change approved by License Amendment No. 244.

Revised License Condition

The revised license condition in Paragraph 2.C.(3) of Renewed FOL No. DPR-46 for CSN would state, in part, that

> NPPD 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 NPPD CSP was approved by License Amendment No. 238 as supplemented by changes approved by License Amendments 244 and 249.

Based on the information in Section 3.0 of this safety evaluation and the modified license condition described above, the NRC staff concludes that the proposed Milestone 8 date is acceptable.

4.0 STATE CONSULTATION

In accordance with the Commission's regulations, the Nebraska 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 of 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. The Commission has previously issued a proposed finding that the amendment involves no significant hazards consideration, and there has been no public comment on such finding published in the *Federal Register* on July 8, 2014 (79 FR 38580). 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

Date: December 12, 2014

January 13, 2015

Mr. Oscar A. Limpias
Vice President-Nuclear and CNO
Nebraska Public Power District
72676 648A Avenue
Brownville, NE 68321

SUBJECT: COOPER NUCLEAR STATION – CORRECTIONS FOR AMENDMENT NO. 249 (TAC NO. MF3631)

Dear Mr. Limpias:

By letter dated December 12, 2014 (Agencywide Documents Access and Management System (ADAMS) Accession No. ML14323A644), the U.S. Nuclear Regulatory Commission (NRC) issued Amendment No. 249 to Renewed Facility Operating License No. DPR-46 for the Cooper Nuclear Station associated with the revised schedule for implementation of the Cyber Security Plan. This amendment was in response to your application dated March 14, 2014, as supplemented by letter dated July 28, 2014. It was discovered that there were some errors in the NRC staff's safety evaluation, however, these errors were minor and did not affect the NRC staff's overall conclusions associated with Amendment No. 249.

Enclosed is the revised safety evaluation to be included with the issued amendment, with revision bars indicating the areas of change. We regret any inconvenience this may have caused.

Sincerely,

/RA/

Siva P. Lingam, Project Manager
Plant Licensing Branch IV-1
Division of Operating Reactor Licensing
Office of Nuclear Reactor Regulation

Docket No. 50-298

Enclosure:
Revised Safety Evaluation

cc w/encl: Distribution via Listserv

DISTRIBUTION:
PUBLIC
LPL4-1 R/F
RidsAcrsAcnw_MailCTR Resource
RidsNrrDorlLpl4-1 Resource
RidsNsirOd Resource
RidsNrrDorlDpr Resource
RidsNrrLAJBurkhardt Resource
RidsNrrPMCooper Resource
RidsRgn4MailCenter Resource
JRycyna, NSIR/CSD

ADAMS Accession No: ML14365A093

OFFICE	NRR/DORL/LPL4-1/PM	NRR/DORL/LPL4-1/LA	NRR/DORL/LPL4-1/BC(A)	NRR/DORL/LPL4-1/PM
NAME	SLingam	JBurkhardt	EOesterle	SLingam
DATE	1/13/15	1/9/15	1/13/15	1/13/15

OFFICIAL RECORD COPY