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

September 8, 2014

Mr. Rafael Flores
Senior Vice President and
Chief Nuclear Officer
Attention: Regulatory Affairs
Luminant Generation Company LLC
P.O. Box 1002
Glen Rose, TX 76043

SUBJECT: COMANCHE PEAK NUCLEAR POWER PLANT, UNIT NOS. 1 AND 2 - ISSUANCE OF AMENDMENTS RE: APPROVAL OF THE REVISED CYBER SECURITY PLAN IMPLEMENTATION SCHEDULE (TAC NOS. MF3216 AND MF3217)

Dear Mr. Flores:

The U.S. Nuclear Regulatory Commission (NRC) has issued the enclosed Amendment No. 163 to Facility Operating License No. NPF-87 and Amendment No. 163 to Facility Operating License No. NPF-89 for Comanche Peak Nuclear Power Plant (CPNPP), Unit Nos. 1 and 2, respectively. The amendments consist of changes to the facility operating licenses in response to your application dated November 21, 2013, as supplemented by letters dated February 4 and April 1, 2014.

The amendments approve the revised schedule for implementation of the cyber security plan (CSP) and revise paragraph 2.H of Facility Operating License Nos. NPF-87 and NPF-89 for CPNPP, Unit Nos. 1 and 2, respectively, to incorporate the revised CSP implementation schedule. The CSP and associated implementation schedule for CPNPP, Unit Nos. 1 and 2, were previously approved by the NRC staff by letter dated July 26, 2011.

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-1
Division of Operating Reactor Licensing
Office of Nuclear Reactor Regulation

Docket Nos. 50-445 and 50-446

Enclosures:
1. Amendment No. 163 to NPF-87
2. Amendment No. 163 to NPF-89
3. Safety Evaluation

cc w/encls: Distribution via Listserv

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

LUMINANT GENERATION COMPANY LLC

COMANCHE PEAK NUCLEAR POWER PLANT, UNIT NO. 1

DOCKET NO. 50-445

AMENDMENT TO FACILITY OPERATING LICENSE

Amendment No. 163
License No. NPF-87

1. The U.S. Nuclear Regulatory Commission (NRC, the Commission) has found that:

   A. The application for amendment by Luminant Generation Company LLC dated November 21, 2013, as supplemented by letters dated February 4 and April 1, 2014, 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, 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.H of Facility Operating License No. NPF-87 is hereby amended to read as follows:

> Luminant Generation Company LLC 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). Luminant Generation Company LLC CSP was approved by License Amendment No. 155, as supplemented by a change approved by License Amendment No. 163.

3. This license amendment is effective as of the date of its issuance and shall be implemented within 90 days from the date of issuance. The full implementation of the CSP shall be in accordance with the implementation schedule submitted by the licensee on November 21, 2013, and approved by the NRC staff with this license amendment. All subsequent changes to the NRC-approved CSP implementation schedule will require prior NRC approval pursuant to 10 CFR 50.90.

FOR THE NUCLEAR REGULATORY COMMISSION

Eric R. Oesterle, Acting Chief
Plant Licensing Branch IV-1
Division of Operating Reactor Licensing
Office of Nuclear Reactor Regulation

Attachment:
Changes to the Facility Operating
License No. NPF-87

Date of Issuance: September 8, 2014

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

LUMINANT GENERATION COMPANY LLC

COMANCHE PEAK NUCLEAR POWER PLANT, UNIT NO. 2

DOCKET NO. 50-446

AMENDMENT TO FACILITY OPERATING LICENSE

Amendment No. 163
License No. NPF-89

1. The U.S. Nuclear Regulatory Commission (NRC, the Commission) has found that:

   A. The application for amendment by Luminant Generation Company LLC dated November 21, 2013, as supplemented by letters dated February 4 and April 1, 2014, 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, 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.H of Facility Operating License No. NPF-89 is hereby amended to read as follows:

> Luminant Generation Company LLC 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). Luminant Generation Company LLC CSP was approved by License Amendment No. 155, as supplemented by a change approved by License Amendment No. 163.

3. This license amendment is effective as of the date of its issuance and shall be implemented within 90 days from the date of issuance. The full implementation of the CSP shall be in accordance with the implementation schedule submitted by the licensee on November 21, 2013, and approved by the NRC staff with this license amendment. All subsequent changes to the NRC-approved CSP implementation schedule will require prior NRC approval pursuant to 10 CFR 50.90.

FOR THE NUCLEAR REGULATORY COMMISSION

Eric R. Oesterle, Acting Chief
Plant Licensing Branch IV-1
Division of Operating Reactor Licensing
Office of Nuclear Reactor Regulation

Attachment:
Changes to the Facility Operating
License No. NPF-89

Date of Issuance: September 8, 2014

ATTACHMENT TO LICENSE AMENDMENT NO. 163

TO FACILITY OPERATING LICENSE NO. NPF-87

AND AMENDMENT NO. 163

TO FACILITY OPERATING LICENSE NO. NPF-89

DOCKET NOS. 50-445 AND 50-446

Replace the following pages of the Facility Operating License Nos. NPF-87 and NPF-89, and Appendix A Technical Specifications with the attached revised pages. The revised pages are identified by amendment number and contain marginal lines indicating the areas of change.

Facility Operating License No. NPF-87

REMOVE	INSERT
8	8

Facility Operating License No. NPF-89

REMOVE	INSERT
8	8

(3) Luminant Generation Company LLC shall promptly notify the NRC of any attempts by subsurface mineral rights owners to exercise mineral rights, including any legal proceeding initiated by mineral rights owners against Luminant Generation Company LLC.

G. Luminant Generation Company LLC shall implement and maintain in effect all provisions of the approved fire protection program as described in the Final Safety Analysis Report through Amendment 78 and as approved in the SER (NUREG-0797) and its supplements through SSER 24, subject to the following provision:

Luminant Generation Company LLC may make changes to the approved fire protection program without prior approval of the Commission only if those changes would not adversely affect the ability to achieve and maintain safe shutdown in the event of a fire.

H. Luminant Generation Company LLC shall fully implement and maintain in effect all provisions of the physical security, guard training and qualification, and safeguards contingency plans, previously approved by the Commission, and all amendments made pursuant to the authority of 10 CFR 50.90 and 10 CFR 50.54(p). The plans, which contain safeguards information protected under 10 CFR 73.21, are entitled: "Comanche Peak Steam Electric Station Physical Security Plan" with revisions submitted through May 15, 2006, with limited approvals as provided for in the Safety Evaluation by the Office of Nuclear Reactor Regulation dated December 5, 2000; "Comanche Peak Steam Electric Station Security Training and Qualification Plan" with revisions submitted through May 15, 2006; and "Comanche Peak Steam Electric Station Safeguards Contingency Plan" with revisions submitted through May 15, 2006. Luminant Generation Company LLC 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). Luminant Generation Company LLC CSP was approved by License Amendment No. 155, as supplemented by a change approved by License Amendment 163.

I. The licensee 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.

J. NOT USED

H. Luminant Generation Company LLC shall fully implement and maintain in effect all provisions of the physical security, guard training and qualification, and safeguards contingency plans, previously approved by the Commission, and all amendments made pursuant to the authority of 10 CFR 50.90 and 10 CFR 50.54(p). The plans, which contain safeguards information protected under 10 CFR 73.21, are entitled: "Comanche Peak Steam Electric Station Physical Security Plan" with revisions submitted through May 15, 2006, with limited approvals as provided for in the Safety Evaluation by the Office of Nuclear Reactor Regulation dated December 5, 2000; "Comanche Peak Steam Electric Station Security Training and Qualification Plan" with revisions submitted through May 15, 2006; and "Comanche Peak Steam Electric Station Safeguards Contingency Plan" with revisions submitted through May 15, 2006. Luminant Generation Company LLC 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). Luminant Generation Company LLC CSP was approved by License Amendment No. 155, as supplemented by a change approved by License Amendment 163.

I. The licensee 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.

J. NOT USED

K. This license is effective as of the date of issuance and shall expire at Midnight on February 2, 2033.

FOR THE NUCLEAR REGULATORY COMMISSION

Original signed by:

Thomas E. Murley, Director
Office of Nuclear Reactor Regulation

Attachments/Appendices:
1. Appendix A - Technical Specifications (NUREG-1468)
1. Appendix B - Environmental Protection Plan
3. Appendix C - Antitrust Conditions

Date of Issuance: April 6, 1993

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

SAFETY EVALUATION BY THE OFFICE OF NUCLEAR REACTOR REGULATION

RELATED TO AMENDMENT NO. 163 TO

FACILITY OPERATING LICENSE NO. NPF-87

AND AMENDMENT NO. 163 TO

FACILITY OPERATING LICENSE NO. NPF-89

LUMINANT GENERATION COMPANY LLC

COMANCHE PEAK NUCLEAR POWER PLANT, UNIT NOS. 1 AND 2

DOCKET NOS. 50-445 AND 50-446

1.0 INTRODUCTION

By application dated November 21, 2013 (Agencywide Documents Access and Management System (ADAMS) Accession No. ML13338A436), as supplemented by letters dated February 4 and April 1, 2014 (ADAMS Accession Nos. ML14051A531 and ML14099A481, respectively), Luminant Generation Company LLC (the licensee) requested changes to the facility operating licenses for Comanche Peak Nuclear Power Plant (CPNPP), Unit Nos. 1 and 2. Portions of letters dated November 21, 2013, and April 1, 2014, respectively, contain sensitive unclassified non-safeguards (security-related) information and, accordingly, those portions are withheld from public disclosure.

The proposed change would revise the date of cyber security plan (CSP) implementation schedule Milestone 8 and the existing license condition 2.H in the facility operating licenses. Milestone 8 of the CSP implementation schedule concerns the full implementation of the CSP. The CSP and associated implementation schedule for CPNPP, Unit Nos. 1 and 2, were previously approved by the U.S. Nuclear Regulatory Commission (NRC) staff by letter dated July 26, 2011 (ADAMS Accession No. ML111780745).

The licensee supplemented the application on February 4, 2014, to provide a public version of the document and, on April 1, 2014, to clarify acronyms used by the licensee throughout the application and to clarify plans for a specific security feature. Hence, the supplements provided additional information that clarified the application, did not expand the scope of the application as originally noticed, and did not change the NRC staff's original proposed no significant hazards consideration determination as published in the *Federal Register* on April 8, 2014 (79 FR 19399).

2.0 REGULATORY EVALUATION

The NRC staff approved the licensee's existing CSP implementation schedule for CPNPP, Unit Nos. 1 and 2, by Amendment No. 155 to Facility Operating License (FOL) NPF-87 and Amendment No. 155 to FOL NPF-89 by letter dated July 26, 2011 (ADAMS Accession No. ML111780745), concurrent with the incorporation of the CSP into the facilities' current licensing bases. By letter dated November 21, 2013, 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:

- 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, 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 include a license condition that requires the licensee to fully implement and maintain in effect all provisions of the Commission-approved CSP (License Condition 2.H for CPNPP, Unit Nos. 1 and 2 FOLs).

- 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[1]), to be considered for evaluating licensees' requests to postpone their cyber security program implementation date (commonly known as Milestone 8).

3.0 TECHNICAL EVALUATION

3.1 Background

The NRC staff issued Amendment No. 155 to FOL NPF-87 for CPNPP, Unit No. 1 and Amendment No. 155 to FOL NPF-89 for CPNPP, Unit No. 2 on July 26, 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 the amendment. The implementation schedule was based on a template prepared by the Nuclear Energy Institute (NEI) (letter dated February 28, 2011; ADAMS Accession No. ML110600206), which the NRC staff found acceptable for licensees to use to develop their CSP implementation schedules by letter dated March 1, 2011 (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);

[1] Internal Memorandum dated October 24, 2013, is a publicly-available document.

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

3) Implement installation of a deterministic one-way device 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 CSP section for 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) Commence ongoing monitoring and assessment activities for those target set CDAs whose security controls have been implemented;

8) Full implementation of the CSP for all safety, security, and emergency preparedness functions.

3.2 Proposed Change

Currently, Milestone 8 of the CPNPP CSP requires the licensee to fully implement the CSP by March 31, 2015. By letter dated November 21, 2013, the licensee has proposed to change the Milestone 8 completion date to June 30, 2017. The licensee has also proposed to modify Paragraph 2.H of FOLs NPF-87 and NPF-89 for CPNPP, Unit Nos. 1 and 2, respectively, to reflect the revised full implementation schedule for the CSP.

3.3 NRC Staff Evaluation

The licensee's request dated November 21, 2013, is consistent with the NRC staff guidance dated October 24, 2013 (ADAMS Accession No. ML13295A467), 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 guidance document 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 guidance document 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 the requirement of the CSP, that it needed additional time to implement, is CSP Section 3.1, "Analyzing Digital Computer Systems and Networks and Applying Cyber Security Controls." The licensee further noted that there are ongoing issues that need resolution prior to completing implementation of Section 3.1. These include NRC and industry discussions about CDAs and security controls; definition of security controls; resource intensive CDA assessment work; the need for careful consideration of remediation activities; change management challenges; and training on new processes, procedures and programs. The NRC staff agrees that implementation of CSP Section 3.1 requires resolution to the technical issues described by the licensee and requires additional time for full implementation of the CSP.

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

The licensee stated it had a project team of 15 to 20 full-time-equivalent (FTE) staff including five Certified Information Systems Security Professionals. It also noted a large number of factors contributing to major challenges with full implementation of Milestone 8. These include a large volume of effort associated with documentation of CDA assessment using the deterministic process in CSP Section 3.1 (more than 600 security controls to be addressed for 2800 CDAs), resulting in a rate of completion of CDA assessments that does not support the current Milestone 8 implementation date. The licensee provided detailed justification for additional time to fully implement the CSP per Section 3.1, quoted below as follows:

a) Resolution of NEI/NRC discussion on critical digital asset (CDA) scope/security controls

- The anticipated resolution time frame does not support the current CPNPP Milestone 8 date.
- Resultant CDA/security controls scope changes will impact Milestone 8 completion.
- Likely scope changes concerning CDA identification and security controls will require significant rework such as:
  - Changes to newly issued procedures and updated existing procedures.
  - Revision of training materials and delivery of training.
  - CDA Assessment Tool rework, programming and validation.
  - Rework to adjust completed CDA assessment work.
  - Rework of the draft Security Controls Implementation Plan (SCIP), which is on-hold pending the outcome of NEI/NRC discussions concerning NEI 13-10, "Cyber Security Control Assessments," Rev 0 [ADAMS Accession No. ML14034A079].

b) Defining the cyber security controls in NEI 08-09 ["Cyber Security Plan for Nuclear Power Reactors,"] Rev. 6 [ADAMS Accession No. ML101180402].

- NEI 10-09, "Addressing Cyber Security Controls for Nuclear Power Reactors," Rev. 0, has not been endorsed by the NRC.
- The anticipated issue date of NUREG 7140 (cyber security controls interpretation guidelines) in late 2013 - leaves limited time to rework the already completed CPNPP SCIP, including reprogramming of the security controls in the cyber security assessment tool.

- Differing industry interpretation of CDA scope and security controls – no defined criteria of "what good looks like" for security controls.

c) CDA Assessment work is resource intensive.

- CPNPP has approximately 2800 CDAs for Units 1 & 2.
- Assessment tool set-up is challenging due to uncertainty surrounding security controls interpretation.
- CPNPP underestimated the level of effort necessary to address security controls using the deterministic criteria in CSP 3.1.6.

d) Remediation activities need to be carefully considered.

- Security controls modifications are unique and new to the plant and suppliers.
- Plant modifications must be carefully implemented to ensure they do not impact plant safety and operation. CPNPP experienced challenges associated with cyber security equipment suppliers' understanding of their own products and limitations; resulting in implementation delays. Suppliers are releasing products that have not been adequately documented and tested which results in corrective action investigations and resource drain.

e) Change management challenges:

- Cyber security is challenging since it integrates into day to day plant operations, maintenance, engineering and procurement activities.
- Integration of cyber security controls is taking longer than expected due to impacts on the work control process and maintenance activities.
- Added burden on maintenance to address security controls validation during maintenance work on CDAs.
- Cyber security for plant CDAs is new, and the security controls being implemented on the plant CDAs are new to Maintenance, System Engineering and Operations. When plant CDA modifications include new products such as application whitelisting, and require operating system parameter changes, the modifications must be implemented cautiously to ensure safe reliable operation of plant equipment. Before modifications are implemented, significant verification analysis and testing must be performed to minimize or eliminate impacts to plant equipment.

- The Work Control Center (WCC) planners are challenged by the nuances associated with cyber security controls. CPNPP is spending additional resources to train the planners to better understand cyber security and how it impacts work planning.
- Maintenance on CDAs is performed by trained and qualified technicians. Training the technicians is a challenge because the maintenance department training schedules are normally established a year in advance and cyber security training requirements are adding a significant amount of emergent training to the schedule.
- Plant modifications that added cyber security controls have created new change management challenges. As cyber security controls are implemented, new tasks are added to normal maintenance activities. The full impact of cyber security controls on the maintenance processes were difficult to predict when plant modifications were initially scoped and developed.

f) Training on new programs, processes and procedures.

- The site training needs and schedules are normally established up to a year in advance and have to be presented to, and approved by, the CPNPP Training Review Boards. Cyber security training adds a new burden on training resources that was not fully understood when the new cyber-related processes and procedures were first being developed. CPNPP initially underestimated the level of effort and coordination needed to meet the requirements of CPNPP's systematic approach to training process. Accommodation of cyber security training needs outside of normal training cycles is an unforeseen burden on training resources.

The NRC staff acknowledges implementation issues with large numbers of CDAs and the need to address many controls for each CDA. However, NEI 13-10 was accepted for use by NRC staff on February 3, 2014 (ADAMS Accession No. ML14031A158). Based on the information provided by the licensee in its application, the NRC staff recognizes that the licensee would not be able to fully implement its CSP at CPNPP, Unit Nos. 1 and 2, by March 31, 2015. As described by the licensee, the CDA assessment work is resource-intensive, and the licensee has a large number of CDAs. The NRC staff agrees remediation activities must be carefully considered and that working with security controls is a new experience for the licensee staff and suppliers, and that security modifications must be implemented to not impact safety and operations. The NRC staff understands that cyber security program implementation has created change management challenges as it has impacted many aspects of the licensee's plant processes including maintenance, engineering, and procurement. The NRC staff

understands that cyber security program implementation has affected long standing training schedules.

Based on the information provided by the licensee, the NRC staff concludes that the licensee has justified the need for additional time for fully implementing the requirements of the cyber security program described above.

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, and stated the revised Milestone 8 date will encompass additional refueling outages, which will provide adequate time to plan and schedule the implementation of design changes identified as a result of the CDA assessments. Additionally, it noted the revised completion date will help to avoid rework that could result from ongoing discussions between NEI and NRC concerning the scope and application of security controls (CSP Section 3.1).

The NRC staff recognizes that delaying final implementation of the cyber security program will provide opportunities to get more work done during outages and avoid rework. Hence, the licensee's proposed completion date is acceptable to the NRC staff.

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 November 21, 2013, the licensee stated, in part, that

> Based on cyber security implementation activities already completed, and completion of activities in progress with a planned completion date of March 31, 2015, CPNPP is secure and will continue to ensure that the digital computer and communication system networks are adequately protected against cyber attacks during implementation of the remainder of the program by the proposed Milestone 8 date of June 30, 2017.

In its letter dated November 21, 2013, the licensee provided the details of the activities completed in each of the Milestones 1 through 7. The activities address significant cyber attack vectors and applied controls to the most risk-significant CDAs.

The NRC staff recognizes that the activities already completed (Milestones 1 through 7), provide a high degree of protection against attacks while the licensee implements the full program at CPNPP, Unit Nos. 1 and 2, by the proposed date of June 30, 2017.

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.

In its letter dated November 21, 2013, the licensee stated, in part, that

> CPNPP methodology for prioritizing Milestone 8 activities is centered on considerations for safety, security, EP [emergency preparedness] and BOP [balance of plant] (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. Prioritization for CDA assessment begins with safety related CDAs and continues through lower priority non-safety and EP CDAs...

The NRC staff concludes that the licensee's methodology is sufficiently conservative and is, therefore, acceptable to the NRC staff.

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

In its letter dated November 21, 2013, the licensee stated that Milestone 1 through 7 activities and other actions implemented by October 29, 2013, provide a high degree of protection against cyber security-related attacks. The licensee noted an effective implementation of the portable media/mobile computing device program and defense-in-depth and installation of diodes between levels. The licensee also has implemented modifications to isolate more significant CDAs from less important CDAs. A Nuclear Oversight audit for all seven interim milestones and on-going Quality Assurance (QA) surveillances under the physical security surveillance program have concluded that the licensee has an effective program. Audit and assessment issues are entered into the corrective action program database and addressed for program improvement. On-going monitoring and time-based periodic actions provide continuing program performance monitoring.

The NRC staff agrees that Milestone 1 through 7 activities including the portable media/mobile computing device program and defense-in-depth and installation of diodes between levels provide significant protection against cyber attacks. Based on the information provided by the licensee, the NRC staff concludes that the licensee is using the quality tools at its disposal to verify the effectiveness of the cyber security program and is addressing issues in its corrective action program (CAP).

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

The licensee stated that the CAP database documents and tracks, from initiation through closure, cyber security actions including issues identified during on-going program assessment activities. The licensee provided the following examples of pending cyber security issues and activities in its CAP:

- Full Program (Milestone 8) implementation tracking
- Milestone 7 periodic and time based on-going action items
- Industry lessons learned for CPNPP cyber security program improvement
- NRC inspection lessons learned for CPNPP cyber security program improvement
- Issues and improvement items identified pertaining to the implemented portions of the cyber security program
- QA surveillance findings
- Pending modifications for Milestone 8
- Operating Experience and pertinent threat release impact evaluations
- Issues documented for program improvements

The NRC staff concludes that the examples reflect the evolution and implementation of the cyber security program and reinforce the licensee discussions above.

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

In its letter dated November 21, 2013, the licensee provided a discussion of completed modifications and pending modifications. The NRC staff concluded that the discussion provided by the licensee describing modifications completed to support the cyber security program and pending cyber security modifications is consistent with the rest of the information described in Section 3.3.

3.4 Revision to License Condition 2.H

By letter dated November 21, 2013, the licensee proposed to modify Paragraph 2.H of Facility Operating License Nos. NPF-87 and NPF-89 for CPNPP, Unit Nos. 1, and 2, respectively, which provides a license condition to require the licensee to fully implement and maintain in effect all provisions of the Commissioned-approved CSP.

The current license condition in Paragraph 2.H of Facility Operating License Nos. NPF-87 and NPF-89 for CPNPP, Unit Nos. 1 and 2, respectively, states, in part:

> Luminant Generation Company LLC 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). Luminant Generation Company LLC CSP was approved by License Amendment No. 155.

The revised license condition in Paragraph 2.H of Facility Operating License Nos. NPF-87 and NPF-89 for CPNPP, Unit Nos. 1 and 2, respectively, would state:

> Luminant Generation Company LLC 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). Luminant Generation Company LLC CSP was approved by License Amendment No. 155, as supplemented by a change approved by License Amendment No. 163.

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

3.5 Summary

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, will 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.

Based on the above, the NRC staff concludes that implementation of Milestones 1 through 7 provides significant protection against cyber attacks; that the licensee's explanation of the need for additional time is justified, and that it is acceptable for CPNPP to complete implementation of Milestone 8, full implementation of the CSP, by June 30, 2017. 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 concludes that the proposed change is acceptable.

4.0 REGULATORY COMMITMENTS

In its letter dated November 21, 2013, the licensee made the following regulatory commitment:

Commitment No.	Commitment	Due Date
3834209	Fully implement the CPNPP Cyber Security Plan for all Safety, Security, and Emergency Preparedness (SSEP) functions.	June 30, 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 Texas State official was notified of the proposed issuance of the amendment. The State official had no comments.

6.0 ENVIRONMENTAL CONSIDERATION

The amendments change a requirement with respect to installation or use of a facility component located within the restricted area as defined in 10 CFR Part 20. The NRC staff has determined that the amendments involve no significant increase in the amounts, and no significant change in the types, of any effluents that may be released offsite, and that there is no significant increase in individual or cumulative occupational radiation exposure. The Commission has previously issued a proposed finding that the amendments involve no significant hazards consideration, and there has been no public comment on such finding published in the *Federal Register* on April 8, 2014 (79 FR 19399). Also, these amendments relate to safeguards matters and do not involve any significant construction impacts or requirements. Accordingly, the amendments meet the eligibility criteria for categorical exclusion set forth in 10 CFR 51.22(c)(9), (10), and (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 amendments.

7.0 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 amendments 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: September 8, 2014

The Notice of Issuance will be included in the Commission's next biweekly *Federal Register* notice.

Sincerely,

/RA/

Balwant K. Singal, Senior Project Manager
Plant Licensing Branch IV-1
Division of Operating Reactor Licensing
Office of Nuclear Reactor Regulation

Docket Nos. 50-445 and 50-446

Enclosures:
1. Amendment No. 163 to NPF-87
2. Amendment No. 163 to NPF-89
3. Safety Evaluation

cc w/encls: Distribution via Listserv

DISTRIBUTION:
PUBLIC
LPL4-1 Reading
RidsAcrsAcnw_MailCTR Resource
RidsNrrDorlDpr Resource
RidsNrrDorlLpl4-1 Resource
RidsNrrPMComanchePeak Resource
RidsNrrLAJBurkhardt Resource
RidsRgn4MailCenter Resource
RidsNsirCsd Resource
JRycyna, NSIR/CSD

ADAMS Accession No.: ML14183A342

OFFICE	NRR/DORL/LPL4-1/PM	NRR/DORL/LPL4-1/LA	NSIR/CSD/D
NAME	BSingal	JBurkhardt	RFelts
DATE	8/1/14	7/8/14	8/6/14
OFFICE	OGC	NRR/DORL/LPL4-1/BC(A)	NRR/DORL/LPL4-1/PM
NAME	CEngland	EOesterle	BSingal
DATE	8/18/14	9/8/14	9/8/14

OFFICIAL AGENCY RECORD