~~SECURITY-RELATED INFORMATION – WITHHOLD FROM PUBLIC DISCLOSURE UNDER 10 CFR 2.390~~

April 29, 2015

ULNRC-06208

U.S. Nuclear Regulatory Commission
Attn: Document Control Desk
Washington, DC 20555-0001

10 CFR 50.90
10 CFR 73.54

Ladies and Gentlemen:

DOCKET NUMBER 50-483
CALLAWAY PLANT UNIT 1
UNION ELECTRIC CO.
RENEWED FACILITY OPERATING LICENSE NPF-30
REQUEST FOR APPROVAL OF A CHANGE TO THE
CALLAWAY PLANT CYBER SECURITY PLAN IMPLEMENTATION DATE
(LICENSE AMENDMENT REQUEST LDCN 15-0009)

References: 1. Letter to Mr. A. Heflin, Union Electric Company, from Mr. Mohan C. Thadani, NRC; "Callaway Plant, Unit 1 - Issuance of Amendment [License Amendment 203] RE: Approval of Cyber Security Plan (TAC No. ME4536)," dated August 17, 2011. (ADAMS Accession No. ML112140087).

Per Reference 1, the NRC approved the Callaway Plant Unit 1 Cyber Security Plan (CSP) and its associated Implementation Schedule. Paragraph 4 of Amendment 203 stated:

Attachment 1 to this letter contains sensitive information.
~~Withhold from public disclosure under 10 CFR 2.390.~~
Upon removal of Attachment 1, this letter is uncontrolled.

~~SECURITY-RELATED INFORMATION – WITHHOLD FROM PUBLIC DISCLOSURE UNDER 10 CFR 2.390~~

> This license amendment is effective as of the date of its issuance. The implementation of the cyber security plan (CSP), including the key intermediate milestone dates and the full implementation date, shall be in accordance with the revised implementation schedule submitted by the licensee on June 29, 2011, 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.

Pursuant to 10 CFR 50.90, "Application for amendment of license or construction permit," Union Electric Company (dba Ameren Missouri), herewith transmits an application for amendment to Renewed Facility Operating License Number NPF-30 for Callaway Plant Unit 1. The license amendment request is for a proposed change to the completion date for Milestone 8 of the CSP implementation schedule.

Attachments 1 through 5 provide the Evaluation of the Proposed Change, Proposed Operating License Change - Marked-Up, Proposed Operating License - Retyped (reflecting the proposed changes), Revised Cyber Security Plan Implementation Schedule, and List of Regulatory Commitments, respectively, in support of this amendment request. Attachment 6 is a redacted version of the Evaluation of the Proposed Change.

It has been determined that this amendment application does not involve a significant hazard consideration as determined per 10 CFR 50.92, "Issuance of amendment." Pursuant to 10 CFR 51.22, "Criterion categorical exclusion or otherwise not requiring environmental review," Section (b), no environmental impact statement or environmental assessment need be prepared in connection with the issuance of this amendment.

This submittal contains a revision to a regulatory commitment to Milestone 8 of the CSP implementation schedule as reflected in Attachment 5.

The Callaway Onsite Review Committee has reviewed and approved the proposed change and has approved the submittal of this amendment application. In addition, in accordance with 10 CFR 50.91 "Notice for public comment; State consultation," Section (b)(1), a copy of this amendment application is being provided to the designated Missouri State official.

Ameren Missouri requests approval of the requested license amendment prior to December 31, 2015. Ameren Missouri further requests that the license amendment be made effective upon NRC issuance, to be implemented within 90 days from the date of issuance.

If there are any questions, please contact Scott Maglio at 573-676-8719.

I declare under penalty of perjury that the foregoing is true and correct.

Sincerely,

Executed on: 4-29-2015

Luke H. Graessle
Senior Director, Operations Support

CSP/nls

Attachments:

1. Evaluation of the Proposed Change
2. Proposed Operating License Change - Marked-Up
3. Proposed Operating License Change - Retyped
4. Revised Cyber Security Plan Implementation Schedule
5. List of Regulatory Commitments
6. Evaluation of the Proposed Change - Redacted Version

cc: Mr. Marc L. Dapas
Regional Administrator
U. S. Nuclear Regulatory Commission
Region IV
1600 East Lamar Boulevard
Arlington, TX 76011-4511

Senior Resident Inspector (w/o Attachment 1)
Callaway Resident Office
U.S. Nuclear Regulatory Commission
8201 NRC Road
Steedman, MO 65077

Mr. Fred Lyon
Project Manager, Callaway Plant
Office of Nuclear Reactor Regulation
U. S. Nuclear Regulatory Commission
Mail Stop O-8B1
Washington, DC 20555-2738

Index and send hardcopy to QA File A160.0761

Hardcopy:

Certrec Corporation
4150 International Plaza Suite 820
Fort Worth, TX 76109
(Certrec receives ALL attachments as long as they are non-safeguards and may be publicly disclosed.)

Electronic distribution without Attachment 1 for the following can be made via Tech Spec ULNRC Distribution:

F. M. Diya
D. W. Neterer
L. H. Graessle
T. E. Herrmann
B. L. Cox
L. H. Kanuckel
S. A. Maglio
T. B. Elwood
Corporate Communications
NSRB Secretary
STARS Regulatory Affairs
Mr. John O'Neill (Pillsbury Winthrop Shaw Pittman LLP)
Missouri Public Service Commission
Ms. Leanne Tippett-Mosby (DNR)

Attachment 2

Proposed Operating License Change - Marked-up

The following text is to be inserted at the end of the Callaway Plant Unit 1 OL Condition 2.E. for Physical Protection:

", as supplemented by changes approved per License Amendment No. XXX."

This marked-up OL change is provided on the next page.

1. In order to ensure that the threads for RPV closure stud hole No. 18 can perform their intended function throughout the period of extended operation, UE shall remove stuck stud No. 18. If repair of stud hole No. 18 is required following removal of the stud, the repair plan shall include inspection of the stud hole prior to and after the completion of the repair.

2. In order to ensure that RPV stud holes with damaged threads can continue to perform their intended function throughout the period of extended operation, UE shall perform a laser inspection for the threads of repaired RPV stud hole location Nos. 2, 4, 5, 7, 9, and 53. If inspection of these RPV stud holes reveals that there is additional degradation in any of these stud holes, the condition will be entered in the Corrective Action Program for evaluation and corrective action, and UE shall also inspect the remaining repaired RPV stud hole locations (Nos. 13, 25, 39 and 54).

D. An Exemption from certain requirements of Appendix J to 10 CFR Part 50, are described in the October 9, 1984 staff letter. This exemption is authorized by law and will not endanger life or property or the common defense and security and are otherwise in the public interest. Therefore, this exemption is hereby granted pursuant to 10 CFR 50.12. With the granting of this exemption the facility will operate, to the extent authorized herein, in conformity with the application, as amended, the provisions of the Act, and the rules and regulations of the Commission.

E. UE shall fully implement and maintain in effect all provisions of the Commission-approved physical security, training and qualification, and safeguards contingency plans including amendments made pursuant to provisions of the Miscellaneous Amendments and Search Requirements revisions to 10 CFR 73.55 (51 FR 27817 and 27822) and to the authority of 10 CFR 50.90 and 10 CFR 50.54(p). The combined set of plans, which contain Safeguards Information protected under 10 CFR 10 CFR 73.21, are entitled: "Callaway Security Plan, Training and Qualification Plan, and Safeguards Contingency Plan, Revision 0" submitted by letter dated October 20, 2004, as supplemented by the letter May 11, 2006.

UE 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 Callaway Plant Unit 1 CSP was approved by License Amendment No. 203, as supplemented by changes approved per License Amendment No. XXX

F. Deleted per Amendment No. 169.

G. UE 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.

Attachment 3

Proposed Operating License Change - Retyped

1. In order to ensure that the threads for RPV closure stud hole No. 18 can perform their intended function throughout the period of extended operation, UE shall remove stuck stud No. 18. If repair of stud hole No. 18 is required following removal of the stud, the repair plan shall include inspection of the stud hole prior to and after the completion of the repair.

2. In order to ensure that RPV stud holes with damaged threads can continue to perform their intended function throughout the period of extended operation, UE shall perform a laser inspection for the threads of repaired RPV stud hole location Nos. 2, 4, 5, 7, 9, and 53. If inspection of these RPV stud holes reveals that there is additional degradation in any of these stud holes, the condition will be entered in the Corrective Action Program for evaluation and corrective action, and UE shall also inspect the remaining repaired RPV stud hole locations (Nos. 13, 25, 39 and 54).

D. An Exemption from certain requirements of Appendix J to 10 CFR Part 50, are described in the October 9, 1984 staff letter. This exemption is authorized by law and will not endanger life or property or the common defense and security and are otherwise in the public interest. Therefore, this exemption is hereby granted pursuant to 10 CFR 50.12. With the granting of this exemption the facility will operate, to the extent authorized herein, in conformity with the application, as amended, the provisions of the Act, and the rules and regulations of the Commission.

E. UE shall fully implement and maintain in effect all provisions of the Commission-approved physical security, training and qualification, and safeguards contingency plans including amendments made pursuant to provisions of the Miscellaneous Amendments and Search Requirements revisions to 10 CFR 73.55 (51 FR 27817 and 27822) and to the authority of 10 CFR 50.90 and 10 CFR 50.54(p). The combined set of plans, which contain Safeguards Information protected under 10 CFR 10 CFR 73.21, are entitled: "Callaway Security Plan, Training and Qualification Plan, and Safeguards Contingency Plan, Revision 0" submitted by letter dated October 20, 2004, as supplemented by the letter May 11, 2006.

UE 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 Callaway Plant Unit 1 CSP was approved by License Amendment No. 203, as supplemented by changes approved per License Amendment No. ###.

F. Deleted per Amendment No. 169.

G. UE shall have and maintain financial protection of such type and in such amounts as the Commission shall require in accordance with Section 170 of the Atomic Energy Act of 1954, as amended, to cover public liability claims.

H. This renewed license is effective as of the date of issuance and shall expire at Midnight on October 18, 2044.

FOR THE NUCLEAR REGULATORY COMMISSION

/RA/

William M. Dean, Director
Office of Nuclear Reactor Regulations

Attachments/Appendices:

1. Attachment 1 (Deleted per Amendment No. 169)
2. Attachment 2 (Deleted per Amendment No. 169)
3. Appendix A - Technical Specifications (NUREG-1058, Revision 1)
4. Appendix B - Environmental Protection Plan
5. Appendix C - Additional Conditions

Date of Issuance: March ____6___, 2015

Attachment 4

Revised Cyber Security Plan Implementation Schedule

Cyber Security Plan Implementation Schedule

Full implementation of the cyber security program involves many supporting tasks. Major activities include: program and procedure development; performing of individual critical digital asset (CDA) assessments; and identification, scheduling, and implementing individual asset security control design remediation actions through the site configuration management program. These design modifications may be performed on-line or could require a refueling outage for installation.

The extensive workload associated with full implementation of the Cyber Security Plan (CSP) requires prioritization to assure those activities that provide higher degrees of protection against radiological sabotage are performed first. Therefore the CSP implementation schedule will be implemented with two major milestone dates. The first milestone date of no later than December 31, 2012, includes the activities listed in the table below. The second milestone date, December 31, 2017, includes the completion of all remaining actions that result in the full implementation of the cyber security plan for all applicable Safety, Security, and Emergency Preparedness (SSEP) functions. This date also bounds the completion of all individual asset security control design remediation actions.

Cyber security controls are not applied if the control adversely impacts safety and important to safety, security or emergency preparedness functions.

#	Implementation Milestone	Completion Date	Basis
1	Establish Cyber Security Assessment Team (CSAT) as described in Section 3.1.2 "Cyber Security Assessment Team" of the Cyber Security Plan (CSP).	No later than December 31, 2012	The CSAT, collectively, will need to have digital plant systems knowledge as well as nuclear power plant operations, engineering and nuclear safety experience and technical expertise. The personnel selected for this team may require additional training in these areas to help ensure adequate capabilities to perform cyber security assessments as well as others duties.
2	Identify Critical Systems (CSs) and Critical Digital Assets (CDAs) as described in Section 3.1.3 "Identification of Critical Digital Assets" of the CSP.	No later than December 31, 2012	The scope of 10 CFR 73.54 includes digital computer and communication systems and networks associated with: safety-related and important-to safety functions; security functions; emergency preparedness functions, including offsite communications; and support systems and equipment which, if compromised, would adversely impact safety, security, or emergency preparedness functions. The scope of 10 CFR 73.54 includes structures, systems, and components (SSCs) that have a nexus to radiological health and safety and therefore can directly or indirectly affect reactivity of a nuclear power plant

#	Implementation Milestone	Completion Date	Basis
			and could result in an unplanned reactor shutdown or transient.
3	Implement Installation of a deterministic one-way device between lower level devices (level 0 1,2) and the higher level devices (level 3,4) as described in Section 4.3, "Defense-In-Depth Protective Strategies" of the CSP. Lower security level devices (level 0, 1, 2 devices) that bypass the deterministic device and connect to level 3 or 4 will be modified to prevent the digital connectivity to the higher level or will be modified to meet cyber security requirements commensurate with the level 3 or 4 devices to which they connect. The design modifications that are not finished by the completion date will be documented in the site configuration management and/or change control program to assure completion of the design modification as soon as possible, but no later than the final implementation date.	No later than December 31, 2012	The implementation of communication barriers protects the most critical SSEP functions from remote attacks on plant systems. Isolating the plant systems from the internet as well as from the corporate business systems is an important milestone in defending against external threats. While the deployment of the barriers is critical to protection from external cyber threats, it also prevents remote access to core monitoring and plant data systems for reactor engineers, plant operations, and other plant staff. This elimination of remote access to reactor core monitoring systems may require the development and execution of a detailed change management plan to ensure continued safe operation of the plants. Vendors may be required to develop software revisions to support the model. The modification will be developed, prioritized and scheduled.
4	The security control "Access Control For Portable And Mobile Devices" described in Appendix D 1.19 of NEI 08-09, Revision 6, will be implemented.	No later than December 31, 2012	Portable media devices are used to transfer electronic information (e.g., data, software, firmware, virus engine updates and configuration information) to and from plant process equipment. Careful use of this class of media is required to minimize the spread of malicious software to plant process equipment. The effective implementation of this control may

#	Implementation Milestone	Completion Date	Basis
			require the coordinated implementation of other complimentary controls to ensure adequate mitigation.
5	Implement observation and identification of obvious cyber related tampering to existing insider mitigation rounds by incorporating the appropriate elements in Appendix E Section 4.3 "Personnel Performing Maintenance And Testing Activities."	No later than December 31, 2012	Insider mitigation rounds by trained staff look for obvious signs of cyber related tampering and would provide mitigation of observable cyber related insider actions. Implementing steps to add signs of cyber security-related tampering to insider mitigation rounds will be performed by the completion date.
6	Identify, document, and implement cyber security controls in accordance with the Cyber Security Plan Section 3.1.6 "Mitigation of Vulnerabilities and Application of Cyber Security Controls" for CDAs that could adversely impact the design function of physical security target set equipment. The implementation of controls that require a design modification that are not finished by the completion date will be documented in the site configuration management and/or change control program to assure completion of the design modification as soon as possible, but no later than the final implementation date.	No later than December 31, 2012	The site physical protection program provides high assurance that these elements are protected from physical harm by an adversary. The cyber security program will enhance the defense-in-depth nature of the protection of CDAs associated with target sets. Implementing Cyber Security Plan security technical controls to target set CDAs provides a high degree of protection against a cyber related attack that could lead to radiological sabotage. Security controls will be addressed in accordance with Cyber Security Plan Section 3.1.6 with the exception of those that require a design modification. Callaway has only a single target set CDA. This CDA is a standalone device with no connectivity. The device is firmware based and can only be accessed locally, with limited user definable parameters. Additional Operational controls will be put into place by December 31, 2012 to mitigate the possibility of locally tampering with the device. This ensures the following are in place for the protection of the target set CDA by December 31, 2012: 1) Deterministic isolation of the CDA

#	Implementation Milestone	Completion Date	Basis
			2) A strong physical security program 3) A process for the handling of portable media 4) An effective insider mitigation program Interim security controls will be implemented under an auditable process to ensure the integrity of the target set CDA's protection by December 31, 2012. Implementation of comprehensive Operational and Management Security Controls will be in accordance with the Callaway cyber security project schedule and are not necessary to ensure protection of the target set CDA.
7	Ongoing monitoring and assessment activities commence, as described in Section 4.4, "Ongoing Monitoring and Assessment" of the CSP, for those target set CDAs whose security controls have been implemented.	No later than December 31, 2012	The ongoing monitoring and assessment activities as described in Section 4.4, "Ongoing Monitoring and Assessment" of the Cyber Security Plan will be implemented for the controls applied to target set CDAs. This action results in the commencement of the cyber security program for target set related CDAs.
8	Full implementation of the Callaway Cyber Security Plan for all SSEP functions will be achieved.	December 31, 2017	By the completion date, the Callaway Cyber Security Plan will be fully implemented for all SSEP functions in accordance with 10 CFR 73.54. This date also bounds the completion of all individual asset security control design remediation actions including those that require a refueling outage for implementation.

Attachment 5

List of Regulatory Commitments

The following table identifies those actions committed to by Ameren Missouri in this document. Any other statements in this submittal are provided for information purposes and are not considered to be regulatory commitments.

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

Attachment 6

Evaluation of Proposed Change – Redacted Version

1.0 SUMMARY DESCRIPTION

This License Amendment Request (LAR) is for a proposed change to the completion date for a milestone in the implementation schedule for the "Cyber Security Plan for Ameren Missouri (Union Electric Company) Callaway Plant Unit 1," (hereafter referred to as the Cyber Security Plan or CSP), including a proposed revision to Paragraph 2.E of the Renewed Facility Operating License (No. NPF-30) for Callaway Plant.

2.0 DETAILED DESCRIPTION

In the Safety Evaluation attached to Reference 1 (page 13), the Cyber Security Plan for Callaway Plant and associated implementation schedule were approved by the Nuclear Regulatory Commission (NRC). Because the CSP implementation schedule contained in Reference 2 was utilized as a basis, in part, for the NRC's safety evaluation provided by Reference 1, NRC approval is being sought for the change(s) proposed herein. Specifically, this amendment request includes: 1) a proposed revision of the CSP implementation schedule in regard to the completion date of Implementation Milestone 8 and 2) a proposed change to the physical protection license condition contained in the Renewed Facility Operating License to reflect the amended CSP implementation schedule. Currently, Implementation Milestone 8 requires full implementation of the Callaway Plant Cyber Security Plan for all SSEP functions (i.e., safety-related and important-to-safety functions, security functions, and emergency preparedness functions including offsite communications) by no later than May 31, 2016. This change proposes a revision to the completion date of Implementation Milestone 8 of December 31, 2017.

To reflect the revised Milestone 8 Implementation date (as proposed), a revised CSP implementation schedule is provided in Attachment 4. Changes are indicated by revision bars on the revised document. The changes include revising the Milestone 8 implementation date wherever it appears (in two places) on the document, as well as the removal of some of the text that was provided in the "Basis" column for Milestone 8 (since that text would no longer be needed in light of the requested extension).

Notwithstanding the changes described above to the CSP implementation schedule, the rest of the schedule contained in Attachment 4 is what was approved in License Amendment No. 203. In regards to Implementation Milestone 6, the basis for the completion date contained the following statement "Callaway has only a single target set CDA." From completion of that activity, and for the purposes of providing complete information, it should be noted that additional target set CDAs (beyond the originally identified single target set CDA) were ultimately identified for Callaway. Appropriate security controls were applied.

3.0 TECHNICAL EVALUATION

In Reference 3, the Nuclear Energy Institute (NEI) transmitted to the NRC an implementation schedule template to aid compliance with the NRC's cyber security regulations codified in 10 CFR 73.54, which was acknowledged in Reference 4 by the NRC. NEI engaged the industry in an effort to ensure that utilities submit an implementation schedule consistent with the template provided by Reference 3. Ameren Missouri provided the requested implementation schedule in Reference 2 in accordance with the NRC-acknowledged template.

As noted above, this proposed change would revise the Implementation Milestone 8 completion date of the Callaway CSP implementation schedule. The current implementation schedule requires Callaway to fully implement the Cyber Security Plan by May 31, 2016. The proposed completion date for Implementation Milestone 8 of the Cyber Security Plan is December 31, 2017.

An NRC memorandum (Reference 7) provides eight criteria for the review of license amendment requests submitted to revise Implementation Milestone 8 dates. The following technical evaluation provides information that addresses those eight criteria. Included in the evaluation is an explanation of the current status of the Callaway cyber security program and the need to revise the Implementation Milestone 8 completion date. The evaluation describes how prioritization of Ameren Missouri's completed and planned implementation actions provides assurance that digital computer and communication systems and networks are adequately protected against cyber attacks including the design basis threat established by 10 CFR 73.1(a)(1)(v).

Boxes show areas of text redacted due to security related information.

Boxes show areas of text redacted due to security related information.

Boxes show areas of text redacted due to security related information.

Boxes show areas of text redacted due to security related information.

Boxes show areas of text redacted due to security related information.

Boxes show areas of text redacted due to security related information.

Boxes show areas of text redacted due to security related information.

Boxes show areas of text redacted due to security related information.

Boxes show areas of text redacted due to security related information.

Boxes show areas of text redacted due to security related information.

4.0 REGULATORY EVALUATION
4.1 APPLICABLE REGULATORY REQUIREMENTS / CRITERIA

10 CFR 73.54 requires licensees to maintain and implement a cyber security plan. Callaway Plant's renewed facility operating license includes a physical protection license condition, i.e., Paragraph 2.E, that requires Callaway Plant to fully implement and maintain in effect all provisions of the Commission-approved cyber security plan, including changes made pursuant to the authority of 10 CFR 50.90 and 10 CFR 50.54(p).

4.2 SIGNIFICANT HAZARDS CONSIDERATION

Pursuant to 50.90, "Application for amendment of license, construction permit, or early site permit," Ameren Missouri is requesting an amendment to the Renewed Facility Operating License No. NPF-30 for the Callaway Plant. This amendment request proposes a change to the Implementation Milestone 8 completion date specified in the Callaway Cyber Security Plan Implementation Schedule.

Ameren Missouri has evaluated the proposed changes using the criteria in 10 CFR 50.92 and has determined that the proposed change does not involve a significant hazards consideration. An analysis of the issue of no significant hazards consideration is presented below:

Criterion 1: The proposed change does not involve a significant increase in the probability or consequences of an accident previously evaluated.

The proposed change is administrative in nature as it only involves extending the timeframe for final implementation of the cyber security plan for Callaway. It involves no change to the intended plan itself. The change does not alter accident analysis assumptions, add any initiators, or affect the function of plant systems or the manner in which systems are operated, maintained, modified, tested, or inspected. The proposed change does not require any plant modifications that affect the performance capability of the structures, systems, and components (SSCs) relied upon to mitigate the consequences of postulated accidents, and has no impact on the probability or consequences of an accident previously evaluated.

Therefore, the proposed changes do not involve a significant increase in the probability or consequences of an accident previously evaluated.

Criterion 2: The proposed change does not create the possibility of a new or different kind of accident from any accident previously evaluated.

The proposed change to the Callaway Cyber Security Plan Implementation Schedule is administrative in nature. This change does not alter accident analysis assumptions, add any initiators, or affect the function of plant systems or the manner in which systems are operated, maintained, modified, tested, or inspected. The proposed change does not require any plant modifications that could introduce new failure modes leading or contributing to a new or different kind of accident.

Therefore, the proposed change does not create the possibility of a new or different kind of accident from any accident previously evaluated.

Criterion 3: The proposed change does not involve a significant reduction in a margin of safety.

Plant safety margins are established through limiting conditions for operation, limiting safety system settings, and safety limits specified in the technical specifications. The proposed change to the Callaway Cyber Security Plan Implementation Schedule is administrative in nature.

Therefore, the proposed change does not involve a significant reduction in a margin of safety.

Based on the above, Ameren Missouri concludes that the proposed change presents no significant hazards consideration under the standards set forth in 10 CFR 50.92(c), and accordingly, a finding of no significant hazards consideration is justified.

4.3 CONCLUSION

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

5.0 ENVIRONMENTAL CONSIDERATION

The proposed amendment is confined to (i) organizational and procedural matters; (ii) modifications to systems used for security and/or materials accountability; (iii) administrative changes; and (iv) review and approval of transportation routes pursuant to 10 CFR 73.37. Accordingly, the proposed amendment meets the eligibility criterion for categorical exclusion set forth in 10 CFR 51.22(c)(12). Therefore, pursuant to 10 CFR 51.22(b), no environmental impact statement or environmental assessment need be prepared in connection with the proposed amendment.

6.0 REFERENCES

1. Letter to Mr. A. Heflin, Union Electric Company, from Mr. Mohan C. Thadani, NRC; "Callaway Plant, Unit 1 -Issuance of Amendment [License Amendment 203] RE: Approval of Cyber Security Plan (TAC No. ME4536)," dated August 17, 2011. (ADAMS Accession No. ML112140087).
2. Reference to Ameren letter transmitting latest implementation schedule for CSP. Letter to the NRC from Stephanie P. Banker, Union Electric Company; "Supplement to Request for Approval of the Cyber Security Plan," dated June 29, 2011. (ADAMS Accession No. ML111801253).
3. Letter from C. E. Earls, NEI, to R. P. Correia, USNRC, "Template for the Cyber Security Plan Implementation Schedule," dated February 28, 2011. (ADAMS Accession No. ML110600211).
4. EA-02-026, "Order Modifying Licenses, Safeguards and Security Plan Requirements," issued February 25, 2002.
5. NEI 08-09, "Cyber Security Plan for Nuclear Power Reactors," Revision 6, April 2010.
6. Memorandum dated July 1, 2013 from B. Westreich, NRC, to T. Blount, NRC, "Enhanced Guidance for Licensee Near-Term Corrective Actions to Address Cyber Security Inspection Findings and Licensee Eligibility for 'Good-Faith' Attempt Discretion."
7. Memorandum dated October 24, 2013, from R. Felts, NRC to B. Westreich, NRC, "Review Criteria for Title 10 of the Code of Federal Regulations Part 73.54, Cyber Security Implementation Schedule Milestone 8 License Amendment Requests." (ADAMS Accession No. ML13295A467)