Ameren MISSOURI

Callaway Plant

April 1, 2011

ULNRC-05778

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

10 CFR 50.90

Ladies and Gentlemen:

DOCKET NUMBER 50-483
CALLAWAY PLANT UNIT 1
UNION ELECTRIC CO.
FACILITY OPERATING LICENSE NPF-30
RESPONSE TO NRC REQUEST FOR ADDITIONAL INFORMATION REGARDING REQUEST FOR APPROVAL OF THE CALLAWAY PLANT CYBER SECURITY PLAN
(LICENSE AMENDMENT REQUEST LDCN 10-0022, TAC NO. ME4536)

References:
1. **AmerenUE Letter ULNRC-05719, "Request for Approval of the Callaway Plant Cyber Security Plan (License Amendment Request LDCN 10-0022)," dated August 12, 2010**
2. **NRC Letter, "Callaway Plant, Unit 1 – Request for Additional Information Regarding Revision to the Facility Operating License and Request for Review and Approval of the Cyber Security Plant (TAC No. ME4536)," dated March 4, 2011**
3. **Ameren Missouri Letter ULNRC-05739, "Update to Notification Letter Designating Callaway Nuclear Plant Unit 1 Station Balance-of-Plant Systems within the Cyber Security Rule Scope, LDCN 10-0022," dated November 29, 2010**

By letter dated August 12, 2010 (Reference 1), Union Electric Company (dba AmerenUE, now Ameren Missouri) submitted a request to amend the Facility Operating License (No. NPF-30) for Callaway Plant Unit 1. Specifically, AmerenUE requested NRC approval of Callaway's Cyber

Attachment 2 to this letter contains sensitive information.
Withhold from public disclosure under 10 CFR 2.390.
Upon removal of Attachment 2 this letter is uncontrolled.

PO Box 620 | Fulton, MO 65251 | AmerenMissouri.com

Security Plan, provided a proposed Cyber Security Plan Implementation Schedule, and included a proposed revision to the Facility Operating License to incorporate the provisions for implementing and maintaining in effect the provisions of the approved Cyber Security Plan. The license amendment request and proposed Cyber Security Plan were developed in concert with other licensees and the Nuclear Energy Institute (NEI) in accordance with a template(s) developed by NEI.

Per Reference 2 the NRC staff requested additional information in regard to the topics of Records Retention, Implementation Schedule, and Scope of Systems. The attachments hereto provide the requested information. For all responses, Ameren Missouri is responding to the RAI questions based on standard responses that were agreed upon between the NEI and the NRC Staff. These RAI responses will require changes in the license amendment request (LAR) for NRC approval of the Callaway Cyber Security Plan. As described in Reference 3, Ameren Missouri noted that it would revise the Callaway Cyber Security Plan submittal to describe jurisdiction of balance-of-plant systems, structures, and components (SSCs). RAI Question 3 and Ameren Missouri's response also addresses the scope of systems.

Ameren Missouri will provide a timely submittal of the updated Callaway Cyber Security License Amendment Request (LAR) on a date that will be agreed upon with the NRC.

The conclusions of the licensing evaluations submitted in Reference 1 remain valid and unchanged. In addition, it should be noted that this letter does not contain new commitments.

If there are any questions regarding this letter or the attached information, please contact me at (573) 676-8719 or Mr. Thomas Elwood at (314) 225-1905.

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

Sincerely,

Executed on: 4/1/2011

Scott A. M

Scott A Maglio
Regulatory Affairs Manager

Attachment 1: Response to NRC Request for Additional Information (RAI) Regarding License Amendment Request LDCN 10-0022

Attachment 2: Callaway Cyber Security Plan Implementation Schedule

EMF

cc:

(copy w/out Attachment 2 except as noted with asterisk*)

U.S. Nuclear Regulatory Commission (Original and 1 copy)*
Attn: Document Control Desk
Washington, DC 20555-0001

Mr. Elmo E. Collins, Jr.*
Regional Administrator
U.S. Nuclear Regulatory Commission
Region IV
612 E. Lamar Blvd., Suite 400
Arlington, TX 76011-4125

Senior Resident Inspector
Callaway Resident Office
U.S. Nuclear Regulatory Commission
8201 NRC Road
Steedman, MO 65077

Mr. Mohan C. Thadani (2 copies)*
Senior Project Manager, Callaway Plant
Office of Nuclear Reactor Regulation
U. S. Nuclear Regulatory Commission
Mail Stop O-8G14
Washington, DC 20555-2738

Mr. James Polickoski*
Project Manager, Callaway Plant
Office of Nuclear Reactor Regulation
U. S. Nuclear Regulatory Commission
Mail Stop O-8B1A
Washington, DC 20555-2738

Index and send hardcopy to QA File A160.0761

Hardcopy:

Certrec Corporation
4200 South Hulen, Suite 422
Fort Worth, TX 76109
(Certrec receives ALL attachments as long as they are non-safeguards and may be publicly disclosed.)

Electronic distribution for the following can be made via Tech Spec ULNRC Distribution:

(electronic copy w/out Attachment 2)
A. C. Heflin
F. M. Diya
C. O. Reasoner III
L. S. Sandbothe
S. A. Maglio
S. L. Gallagher
T. L. Woodward (NSRB)
T. B. Elwood
E. M. Fast
A. M. Lowry
E. A. Wildgen
Ms. Diane M. Hooper (WCNOC)
Mr. Tim Hope (Luminant Power)
Mr. Ron Barnes (APS)
Mr. Tom Baldwin (PG&E)
Mr. Wayne Harrison (STPNOC)
Ms. Linda Conklin (SCE)
Mr. John O'Neill (Pillsbury Winthrop Shaw Pittman LLP)
Missouri Public Service Commission
Mr. Dru Buntin (DNR)

RESPONSE TO NRC REQUEST FOR ADDITIONAL INFORMATION (RAI)
REGARDING LICENSE AMENDMENT REQUEST LDCN (10-0022)

By letter dated August 12, 2010 (Agencywide Documents Access and Management System (ADAMS) Accession No. MLL102250075), Union Electric Company (the licensee) submitted a request for revision to the Facility Operating License No. NPF-30 and review and approval of the Cyber Security Plan (CSP) for Callaway Plant, Unit 1, in accordance with Title 10 of the *Code of Federal Regulations* (10 CFR), Section 73.54, "Protection of digital computer and communication systems and networks."

The U.S. Nuclear Regulatory Commission (NRC) staff has reviewed the information provided in your application and determined that the following additional information is required in order to complete its review.

Question 1: Records Retention

The regulations in 10 CFR 73.54(c)(2) requires licensees to design a cyber security program to ensure the capability to detect, respond to, and recover from cyber attacks. Furthermore, 10 CFR 73.54(e)(2)(i) requires licensees to maintain a CSP that describes how the licensee will maintain the capability for timely detection and response to cyber attacks. The ability for a licensee to detect and respond to cyber attacks requires accurate and complete records and is further supported by 10 CFR 73.54(h), which states that the licensee shall retain all records and supporting technical documentation required to satisfy the requirements of 10 CFR Section 73.54 as a record until the Commission terminates the license for which the records were developed, and shall maintain superseded portions of these records for at least 3 years after the record is superseded, unless otherwise specified by the Commission.

The licensee's CSP in Section 4.13 states that Critical Digital Asset (CDA) audit records and audit data (e.g., operating system logs, network device logs) are retained for a period of time that is less than what is required by 10 CFR 73.54(h).

Please explain the deviation from the 10 CFR 73.54(h) requirement to retain records and supporting technical documentation until the Commission terminates the license (or to maintain superseded portions of these records for at least 3 years) and how that meets the requirements of 10 CFR 73.54.

Response 1:

Ameren Missouri will revise the License Amendment Request for approval of the Callaway Cyber Security plan by replacing Section 4.13 of the proposed Cyber Security Plan, "Document Control and Records Retention and Handling," with a new Section 4.13 that was developed through discussions between the NEI and NRC staff and approved by the NRC on March 1, 2011 in docketed correspondence to the NEI (ADAMS Accession No. ML110490337). The revision to the Callaway Cyber Security Plan will not deviate from the agreed upon revision and is shown below (next page).

4.13 Document Control And Records Retention And Handling

Ameren Missouri has established the necessary measures and governing procedures to ensure that sufficient records of items and activities affecting cyber security are developed, reviewed, approved, issued, used, and revised to reflect completed work.

The following are examples of records or supporting technical documentation that are retained as a record until the Commission terminates the license for which the records are developed. Superseded portions of these records are retained for three years unless otherwise specified by the Commission, in accordance with the requirements of 10 CFR 73.54(h).

- Modification records for CDAs;
- Analyses, basis, conclusions, and determinations used to establish a component as a CDA;
- Cyber Security Plan;
- Written Policies and Procedures that implement and maintain the Cyber Security program, with records of changes;
- Corrective Action records related to Cyber Security non-conformance or adverse conditions;
- Documentation of periodic Cyber Security Program reviews and Program audits;
- Vulnerability notifications determined to adversely impact CDAs and the associated analyses, assessments and dispositions;
- Training records to document personnel qualifications and program implementation and maintenance; and
- Audit records are electronic or manual event records (logs) that facilitate the identification and analysis of cyber security attacks and are developed in accordance with Appendix D, Section 2, *Audit and Accountability.*
    - The scope of auditable events is developed in accordance with Appendix D, Section 2.2, *Auditable Events.* Events identified for auditing are recorded in accordance with Appendix D, Section 2.3, *Content of Audible Events* and Appendix D, Section 2.4, *Audit Storage Capacity* (for electronic audit records). The source of auditable events (electronic and non-electronic) include, but are not limited to:
        - Operating system logs
        - Service and application logs
        - Network device logs
        - Access Logs
    - Audit records of auditable events are retained to document access history, as well as to discover the source of cyber attacks or other security-related incidents affecting CDAs or SSEP functions, or both. These records are reviewed and analyzed accordance with [policies, procedures, programs] implementing Appendix D, Section 2.6, *Audit Review, Analysis and Reporting.* The review and analysis is conducted consistent with maintaining high assurance that digital computer and communication systems and networks are adequately protected against cyber attacks, up to and including the design basis threat as described in 10 CFR 73.1. Superseded records (or portions thereof) are then retained for three years, after the record has been reviewed and analyzed.

Question 2: Implementation Schedule

The regulations in 10 CFR 73.54 require licensees to submit a CSP that satisfies the requirements of this section for Commission review and approval. Furthermore, each submittal must include a proposed implementation schedule, and the implementation of the licensee's cyber security program must be consistent with the approved schedule. Paragraph 73.54(a) of 10 CFR requires licensees to provide high assurance that digital computer and communication systems and networks are adequately protected against cyber attacks, up to and including the design basis threat.

The completion of several key intermediate milestones (items (a) through (h) below) would demonstrate progress toward meeting the requirements of 10 CFR 73.54. The NRC staff's expectation is that the key intermediate milestones will be completed in a timely manner, but no later than December 31, 2012. The key CSP implementation milestones are as follows:

(a) Establish, train and qualify Cyber Security Assessment Team, as described in Section 3.1.2, "Cyber Security Assessment Team," of the CSP.

(b) Identify Critical Systems and CDAs, as described in Section 3.1.3, "Identification of Critical Digital Assets," of the CSP.

(c) Implement cyber security defense-in-depth architecture by installation of [deterministic one-way] devices, as described in Section 4.3, "Defense-In-Depth Protective Strategies," of the CSP.

(d) Implement the management, operational and technical cyber security controls that address attacks promulgated by use of portable media, portable devices, and portable equipment as described in Appendix D, Section 1.19, "Access Control for Portable and Mobile Devices," of Nuclear Energy Institute (NEI) 08-09, Revision 6.

(e) Implement observation and identification of obvious cyber related tampering to existing insider mitigation rounds as described in Appendix E, Section 4.3, "Personnel Performing Maintenance and Testing Activities," and Appendix E, Section 10.3, "Baseline Configuration," of NEI 08-09, Revision 6.

(f) Identify, document, and implement cyber security controls to physical security target set CDAs in accordance with Section 3.1.6, "Mitigation of Vulnerabilities and Application of Cyber Security Controls," of the CSP.

(g) Ongoing monitoring and assessment activities will commence for those target set CDAs whose security controls have been implemented, as described in Section 4.4, "Ongoing Monitoring and Assessment," of the CSP.

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

Please provide a revised CSP implementation schedule that identifies the appropriate milestones, completion dates, supporting rationale, and level of detail to allow the NRC to evaluate the licensee's

proposed schedule and associated milestone dates which include the final completion date. It is the NRC's intention to develop a license condition incorporating your revised CSP implementation schedule containing the key milestone dates.

Response 2:

Ameren Missouri will revise the License Amendment Request for approval of the Callaway Cyber Security Plan by replacing the current Callaway Cyber Security Plan Implementation Schedule with a new Callaway Cyber Security Plan Implementation Schedule. The new implementation schedule is based on an implementation schedule that was developed through discussions between the NEI and NRC staff and approved by the NRC on March 1, 2011 in docketed correspondence to the NEI (ADAMS Accession No. ML110070348). The revised Callaway Cyber Security Plan Implementation Schedule, which addresses the new requirements and dates outlined in RAI #2 above, is provided in Attachment 2.

Question 3: Scope of Systems

Paragraph 73.54(a) of 10 CFR requires licensees to provide high assurance that digital computer and communication systems and networks are adequately protected against cyber attacks, up to and including the design basis threat as described in 10 CFR 73.1. In addition, 10 CFR 73.54(a)(1) states that

> The licensee shall protect digital computer and communication systems and networks associated with:
>
> (i) Safety-related and important-to-safety functions;
>
> (ii) Security functions;
>
> (iii) Emergency preparedness functions, including offsite communications; and
>
> (iv) Support systems and equipment which, if compromised, would adversely impact safety, security, or emergency preparedness functions.

Subsequent to the issuance of the cyber security rule, the NRC stated that 10 CFR 73.54 should be interpreted to include structures, systems, and components (SSCs) in the balance-of-plant (BOP) that have a nexus to radiological health and safety (ADAMS Accession No. ML103490344, dated November 19, 2010). The SSCs in the BOP are those that could directly or indirectly affect reactivity of a nuclear power plant and could result in an unplanned reactor shutdown or transient and are therefore within the scope of important-to-safety functions described in 10 CFR 73.54(a)(1). Furthermore, the NRC issued a letter to NEI dated January 5, 2011 (ADAMS Accession No. ML103550480) that provided licensees with additional guidance on one acceptable approach to comply with the Commission's policy determination.

Please explain how the scoping of systems provided by CSP for Callaway Plant, Unit 1 meet the requirements of 10 CFR 73.54 and the additional guidance provided by the NRC.

Response 3:

Ameren Missouri will revise the License Amendment Request for approval of the Callaway Cyber Security Plan by inserting a new paragraph into section 2.1 of the Cyber Security Plan. The text of this paragraph was developed by NRC staff and approved by the NRC on January 5, 2011 in docketed correspondence to the NEI (Accession No. ML103550480). The revision to the Callaway Cyber Security Plan will not deviate from the identified text and is shown below.

"Within the scope of NRC's cyber security rule at Title 10 of the Code of Federal Regulations (10 CFR) 73.54, systems or equipment that perform important to safety functions include structures, systems, and components (SSCs) in the balance of plant (BOP) that could directly or indirectly affect reactivity at a nuclear power plant and could result in an unplanned reactor shutdown or transient. Additionally, these SSCs are under the licensee's control and include electrical distribution equipment out to the first inter-tie with the offsite distribution system."