



Callaway Plant

December 30, 2010

ULNRC-05758

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
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. Electronic Request for Additional Information (RAI) from NRC dated November 30, 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 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 provisions or requirements of a particular section within the proposed Cyber Security Plan. The attachment hereto provides the requested information.

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.

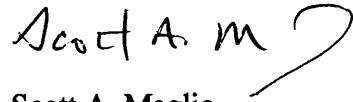
ULNRC-05758
December 30, 2010
Page 2

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: 12/30/2010.


Scott A. Maglio
Regulatory Affairs Manager

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

EMF

cc: 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:

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**

Question:

Title 10 of the *Code of Federal Regulations* (10 CFR) 73.54(b)(1) requires licensees to analyze digital computer and communication systems and networks, and identify those assets that must be protected against cyber attacks. 10 CFR 73.54(e)(1) requires that the cyber security plan must describe how the requirements of this section will be implemented and must account for the site-specific conditions that affect implementation.

The Callaway Plant, Unit 1, Cyber Security Plan (CSP), Section 3.1.5, "Tabletop Reviews and Validation Testing," describes tabletop review and validation activities for the Cyber Security Assessment Team. The CSP further states that the "activities are validated for Critical Digital Assets through a combination of table top reviews and walk-downs."

The purpose of performing physical and electronic walk-downs is to validate that available plant documentation is up to date, accurate and comprehensive. Thus, a walk down, unlike a table top review, can identify and correct documentation issues found by the walkdowns.

Explain the conditions under which the Licensee will use table top reviews rather than conducting actual walk-downs. Please fully identify and document networks and site-specific conditions, to provide assurance that the table top reviews will provide an acceptable level of confidence in validation as the walk-downs would.

Response:

For context, the referenced section is copied below. The text where Ameren deviated from the NEI template is underlined. The sentence containing that text is the subject of the RAI and this response. (Note: "CDA" in the text below is short for "critical digital asset.")

3.1.5 Tabletop Reviews and Validation Testing

The CSAT conducts a tabletop review and validation activities.

Results of table top reviews and validation reviews are documented.

For each CDA/CDA group, the CSAT:

- Confirms the location;
- Confirms direct and indirect connectivity pathways;
- Confirms infrastructure interdependencies;
- Reviews any CDA assessment documentation;
- Reviews the defensive strategies;

- Reviews the defensive models;
- Confirms the implementation of plant-wide physical and cyber security policies and procedures that secure the CDAs from a cyber attack, including attack mitigation, and incident response and recovery;
- Confirms that staff members working with the CDAs are trained to a level of cyber security knowledge commensurate with their assigned responsibilities; and
- Identifies and documents the CDA cyber security exposures including specific attack/threat vectors to be assessed for mitigation using the method in Section 3.1.6.

The above activities are validated for CDAs through a combination of table top reviews and walk-downs.

Ameren intends to physically walk-down every CDA in accordance with NRC expectations. Ameren believes, however, that it is not possible to validate some items in the above list by doing a physical walk-down. Some validation items, such as confirming that staff members working with the CDAs have the proper training, can only be validated by table top or document review. Ameren therefore attempted to clarify that this validation would require some documentation reviews in addition to physical walk-downs. This was not intended as an “or” statement and Ameren did not plan to perform table top reviews in lieu of walk-downs on any systems. Consequently, no networks or site-specific conditions need to be identified and no justification is required to assure that a table top review will provide the same level of confidence as a physical walk-down.