Ameren
MISSOURI

Callaway Plant

June 28, 2011

ULNRC-05802

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

10 CFR 73.22(f)(3)

Ladies and Gentlemen:

DOCKET NUMBER 50-483
CALLAWAY PLANT UNIT 1
UNION ELECTRIC CO.
FACILITY OPERATING LICENSE NPF-30
REQUEST FOR APPROVAL OF SECURE VOICE COMMUNICATIONS
CCORE MODULE BY CELLCRYPT LIMITED

Reference: 1. Title 10, Code of Federal Regulations Part 73.22(f)(3)
2. National Institute of Standards and Technology (NIST) Cryptographic Module Validation Program (CMVP)

Pursuant to 10 CFR 73.22(f)(3) (Ref. 1), Union Electric Company (dba Ameren Missouri) hereby requests approval to utilize mobile telephone devices to transmit safeguards information using the Cellcrypt Mobile application and the CCORE Cryptographic Module by Cellcrypt Limited. This module meets the requirements of FIPS 140-2 per the latest validation list of Reference 2. Validation certificate No. 1310 for subject module is enclosed.

This communication contains no new licensing basis commitments by Ameren Missouri.

Should you have any questions, please contact Kenny Weith at (573) 676-6111.

Sincerely,

Kevin Bruckerhoff
Assistant Manager, Protective Services

EMF

Enclosure: FIPS 140-2 Validation Certificate No. 1310 for CCORE Module by Cellcrypt Limited

cc: 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 630
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 Responses and Reports ULNRC Distribution:

A. C. Heflin
F. M. Diya
C. O. Reasoner III
L. H. Graessle
S. M. Maglio
T. B. Elwood
S. L. Gallagher
K. R. Weith
NSRB Secretary
Mr. Paul Parmenter, Director (SEMA)
Mr. Thomas Mohr, Senior REP Planner (SEMA)
Mr. John Campbell, REP Planner (SEMA)
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)
Mr. Dru Buntin (DNR)

FIPS 140-2 Validation Certificate

The National Institute of Standards and Technology of the United States of America

The Communications Security Establishment of the Government of Canada

FIPS 140-2 TM

Certificate No. **1310**

The National Institute of Standards and Technology, as the United States FIPS 140-2 Cryptographic Module Validation Authority; and the Communications Security Establishment, as the Canadian FIPS 140-2 Cryptographic Module Validation Authority; hereby validate the FIPS 140-2 testing results of the Cryptographic Module identified as:

CCORE Module *by* Cellcrypt Limited

in accordance with the Derived Test Requirements for FIPS 140-2, Security Requirements for Cryptographic Modules. FIPS 140-2 specifies the security requirements that are to be satisfied by a cryptographic module utilized within a security system protecting *Sensitive Information* (United States) or *Protected* Information (Canada) within computer and telecommunications systems (including voice systems).

Products which use the above identified cryptographic module may be labeled as complying with the requirements of FIPS 140-2 so long as the product, throughout its life cycle, continues to use the validated version of the cryptographic module as specified in this certificate. The validation report contains additional details concerning test results. No reliability test has been performed and no warranty of the products by both agencies is either expressed or implied.

This certificate includes details on the scope of conformance and validation authority signatures on the reverse.

FIPS 140-2 provides four increasing, qualitative levels of security: Level 1, Level 2, Level 3, and Level 4. These levels are intended to cover the wide range and potential applications and environments in which cryptographic modules may be employed. The security requirements cover eleven areas related to the secure design and implementation of a cryptographic module. The scope of conformance achieved by the cryptographic modules as tested in the product identified as:

CCORE Module *by* Cellcrypt Limited
(Software Version: 0.6.0-rc3;* Software*)

and tested by the Cryptographic Module Testing accredited laboratory: ***CEAL: a CygnaCom Solutions Laboratory, NVLAP Lab Code 200002-0***
CRYPTIK Version 7.0

is as follows:

Cryptographic Module Specification:	Level 1	*Cryptographic Module Ports and Interfaces:*	Level 1
Roles, Services, and Authentication:	Level 1	*Finite State Model:*	Level 1
Physical Security: *(Multi-Chip Standalone)*	Level N/A	*Cryptographic Key Management:*	Level 1
EMI/EMC:	Level 1	*Self-Tests:*	Level 1
Design Assurance:	Level 1	*Mitigation of Other Attacks:*	Level N/A
Operational Environment:	Level 1	*tested in the following configuration(s):*	Ubuntu Server

The following FIPS approved Cryptographic Algorithms are used: **AES (Cert. #1089); RSA (Cert. #514); SHS (Cert. #1022); HMAC (Cert. #612); RNG (Cert. #611)**

The cryptographic module also contains the following non-FIPS approved algorithms: **RSA (key wrapping; key establishment methodology provides 112 bits of encryption strength); RC4; MD5; EC Diffie-Hellman (non-compliant); ECDSA (non-compliant)**

Overall Level Achieved: 1

Signed on behalf of the Government of the United States

Signature: Donna F. Dodson

Dated: May 19, 2010

Chief, Computer Security Division
National Institute of Standards and Technology

Signed on behalf of the Government of Canada

Signature:

Dated: May 10, 2010

Director, Industry Program Group
Communications Security Establishment Canada