

January 7, 2005

U.S. Nuclear Regulatory Commission
Attn: Document Control Desk
Mail Stop P1-137
Washington, DC 20555-0001

ULNRC05111
TAC No. MC2899



Ladies and Gentlemen:

**DOCKET NUMBER 50-483
CALLAWAY PLANT UNIT 1
UNION ELECTRIC CO.
FACILITY OPERATING LICENSE NPF-30
USE OF ENCRYPTION SOFTWARE FOR ELECTRONIC TRANSMISSION
OF SAFEGUARDS INFORMATION**

References: 10CFR73.21 and NRC Regulatory Issue Summary 2002-15

Pursuant to the requirements of 10 CFR 73.21(g)(3), Union Electric requests approval to process and transmit Safeguards Information (SGI) using PGP Software (Enterprise, Corporate, or Personal) Desktop Version 8.0 or the latest validated version, developed with PGP SDK 3.0.3. National Institute of Standards and Technology Certificate 394 validates compliance of this SDK with FIPS 140-2 requirements.

An information protection system for SGI that meets the requirements of 10 CFR 73.21(b) through (i) has been established and is being maintained. Prior to the first use of encryption software for SGI material, written procedures shall be in place to describe, as a minimum: access controls; where and when encrypted communications can be made; how encryption keys, codes and passwords will be protected from compromise; actions to be taken if the encryption keys, codes or passwords are, or are suspected to have been, compromised (for example, notification of all authorized users); and how the identity and access authorization of the recipient will be verified.

Union Electric intends to exchange SGI with the NRC, Nuclear Energy Institute (NEI), and other SGI holders who have received NRC approval to use PGP software. Michael O. McCrady, Network Project Integrator, is responsible for the overall implementation of the SGI encryption program at Union Electric. Michael O. McCrady, Network Project Integrator, is responsible for collecting, safeguarding, and disseminating the software tools needed for encryption and decryption of SGI.

ULNRC05111
January 7, 2005
Page 2

Pursuant to 10 CFR 73.21(g)(3), the transmission of encrypted material to other authorized SGI holders, who have received NRC approval to use PGP software, would be considered a protected telecommunications system. The transmission and dissemination of unencrypted SGI is subject to the provisions of 10 CFR 73.21(g)(1) and (2).

If you have any questions concerning this matter please contact Mr. Mark Dunbar at (573) 676-4205.

Sincerely,

A handwritten signature in black ink, appearing to read "Luke H. Graessle".

Luke H. Graessle
Superintendent, Protective Services

LHG/rg

ULNRC05111
January 7, 2005
Page 3

cc: Mr. Bruce S. Mallett (2 copies)
Regional Administrator
U.S. Nuclear Regulatory Commission
Region IV
611 Ryan Plaza Drive, Suite 400
Arlington, TX 76011-4005

Physical Security Inspector
U.S. Nuclear Regulatory Commission
611 Ryan Plaza Drive, Suite 400
Arlington, TX 76011-4005

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

Mr. Jack N. Donohew (2 copies)
Licensing Project Manager, Callaway Plant
Office of Nuclear Reactor Regulation
U. S. Nuclear Regulatory Commission
Mail Stop 7E1
Washington, DC 20555-2738

Missouri Public Service Commission
Governor Office Building
200 Madison Street
PO Box 360
Jefferson City, MO 65102-0360

U.S. Nuclear Regulatory Commission
Attn: Scott Morris, NRC/NISR
11545 Rockvill Pike
Rockville, MD 20852

U.S. Nuclear Regulatory Commission
Attn: Lynn Silvius, NRC/NSIR
11555 Rockvill Pike
Rockville, MD 20852

U.S. Nuclear Regulatory Commission
Attn: Louis Grosman, NRC/OCIO
11545 Rockvill Pike
Rockville, MD 20852

Nuclear Energy Institute
Attn: James Davis
1776 I Street, NW, Suite 400
Washington, D.C. 20006-3708

SDP-ZZ-00001

USE OF PGP ENCRYPTION SOFTWARE

Revision: 000

USE OF PGP ENCRYPTION SOFTWARE**TABLE OF CONTENTS**

<u>Section</u>	<u>Page Number</u>
1.0 PURPOSE	3
2.0 SCOPE	3
3.0 RESPONSIBILITIES.....	3
3.1. Protective Services Security Supervisor	3
3.2. Authorized SGI Encryption User	3
4.0 PROCEDURE INSTRUCTIONS	4
4.1. SGI Computers and Printers.....	4
4.2. Use of Encryption Software	4
4.3. E-Mail Transmission of Encrypted Files.....	5
4.4. Decryption of Encrypted Files	5
5.0 REFERENCES.....	6
5.1. Implementing	6
5.2. Developmental	6
6.0 RECORDS	6
7.0 DEFINITIONS.....	6
8.0 SUMMARY OF CHANGES	7

USE OF PGP ENCRYPTION SOFTWARE

1.0 PURPOSE

- 1.1. The purpose of this procedure is to identify the requirements for the use of Pretty Good Privacy (PGP) encryption software for management and transmission of Safeguards Information (SGI).

2.0 SCOPE

- 2.1. This procedure provides guidance for the encryption, management, and electronic transmission of sensitive security information, including SGI, between Callaway Plant and other authorized PGP users.
- 2.2. This procedure provides a standardized approach that will allow effective encryption and electronic exchange of SGI information.
- 2.3. PGP Corporation Software, latest FIPS 140 validated version is used.

3.0 RESPONSIBILITIES

3.1. Protective Services Security Supervisor

- 3.1.1. Implements the SGI encryption program described in this procedure.
- 3.1.2. Ensures individuals have an appropriate safeguards clearance prior to receiving access to a key or pass-phrase used for encryption or decryption of SGI.
- 3.1.3. Ensures individuals have appropriate user level knowledge of PGP software procedures prior to being granted permission to encrypt and electronically transmit SGI.
- 3.1.4. Grants individual permission to encrypt and transmit SGI, and maintains a list of authorized users.
- 3.1.5. Notifies public key holders if a pass-phrase, keypair, has been, or is suspected of being, compromised.

3.2. Authorized SGI Encryption User

Notifies the Protective Services Security Supervisor when a pass-phrase, keypair, or electronic file has been, or is suspected of being, compromised.

-END OF SECTION-

4.0 PROCEDURE INSTRUCTIONS

4.1. SGI Computers and Printers

- 4.1.1. SGI may be processed or stored in unencrypted form on computer systems provided that the systems are self-contained stand alone and not connected to a network with non-safeguards access (LAN).
- 4.1.2. WHEN processing unencrypted SGI the computer is NOT left unattended and is controlled as SGI material.
- 4.1.3. SGI may only be printed on a stand alone printer.
- 4.1.4. Printers used to print SGI are treated as uncontrolled if a determination can be made that the memory is free of SGI after printing is completed OR the unit powered down.

-END OF SECTION-

4.2. Use of Encryption Software

4.2.1. Encryption Keypairs

- a. GENERATE keypairs using a multi-word pass-phrase which contains alphanumeric characters, at least one of which should be a number.
- b. PROTECT the private key pass-phrase as SGI.
- c. Public keys are NOT SGI. Do NOT post public keys to a keyserver.
- d. INCLUDE the key owner's name and company in the keypair full name.

4.2.2. Exchange of Public Keys

- a. PROVIDE the public key to authorized users on electronic media, such as a disk, or CD-Rom.
- b. PROVIDE the appropriate e-mail address that corresponds to the key owner.
- c. Prior to use, the receiving organization CONFIRMS that the key is from an authorized individual by:
 - 1. ENSURING that the key was provided by the individual listed on the key.
 - 2. ENSURING that the individual is authorized access to SGI by determining a "need to know".

4.2.3. SGI encryption users MAINTAIN a list of individuals to whom the public key has been provided using the Authorized SGI Encryption User List.

4.2.4. The individuals on the Authorized SGI Encryption User List are promptly notified if the pass-phrase, keypair, has been, or is suspected of being, compromised.

-END OF SECTION-

4.3. E-Mail Transmission of Encrypted Files

- 4.3.1. USING the appropriate public keys, ENCRYPT files on a properly protected computer prior to transmission.
- 4.3.2. Prior to sending the encrypted file, VERIFY that the file is encrypted by confirming the addition of ".pgp" to the file extension.

CAUTION

Do NOT attach the unencrypted version of a file on the memory device used during this transfer process.

- 4.3.3. USE a memory device, disk, CD, etc. to transfer the encrypted file to an unprotected network computer for attachment to an e-mail.
- 4.3.4. Encrypted files may be sent as e-mail attachments to the appropriate addressees.

4.4. Decryption of Encrypted Files

- 4.4.1. Prior to decryption of the file, recipients move the encrypted e-mail attachment to a properly protected safeguards computer.
- 4.4.2. DECRYPT the file using the private key pass-phrase.

-END OF SECTION-

5.0 REFERENCES

5.1. Implementing

5.1.1. APA-ZZ-00204, Safeguards Information

5.2. Developmental

5.2.1. 10 CFR 73.21 (Requirements for the protection of safeguards information.)

5.2.2. NRC Regulatory Issue Summary 2002-15, 08/28/2002.

6.0 RECORDS

6.1. Authorized SGI Encryption User List (Maintained by the Security Clerk)

6.2. Public Key Distribution List (Maintained by the Security Clerk)

7.0 DEFINITIONS

7.1. Keypair – A Public Key and a Private Key that are created for the purpose of the encryption/decryption of SGI.

7.2. Keyserver – A server on the LAN or internet that collects and distributes public keys.

7.3. Private Key – A key (pass-phrase) used by the public key holder/owner to decrypt information that was encrypted with the corresponding public key.

7.4. Public Key – A key that is generated to enable another individual to encrypt information for the purpose of transmitting the information to the public key holder/owner.

8.0 SUMMARY OF CHANGES

Page(s)	Section or Step Number	Description