USE OF PGP ENCRYPTION SOFTWARE FOR MANAGEMENT AND TRANSMISSION OF SAFEGUARDS INFORMATION

MARCH 26, 2004

1 SCOPE

This procedure provides guidance for the encryption, management, and electronic transmission of sensitive security information, up to Safeguards Information (SGI) between power reactor licensees, materials licensees with safeguards programs, the Nuclear Regulatory Commission (NRC) and Nuclear Energy Institute (NEI). This procedure provides a standardized approach that will allow effective encryption and electronic exchange of SGI information.

PGP Corporation Software, latest FIPS 140 validated ~~V~~version ~~8.0, or later~~, shall be used. Each licensee is responsible for obtaining an appropriate software license~~s~~ and installation of PGP software in accordance with manufacturers instructions.

This procedure addresses how provisions of 10 CFR 73.21(~~f~~g)(3) will be met using the selected encryption system. ~~Licensees who follow this procedure do not need individual authorization from the NRC~~.

~~This procedure does not address licensee responsibility for control, storage, of hard copy SGI material or word processing equipment where encryption is not being used.~~

2 DISCUSSION

The use of protected electronic communications for transmittal of SGI between licensees and the NRC, and NEI will enable more effective administration and control of security programs. To allow efficient exchange of encrypted information within the industry a single, standard~~,~~ approach must be followed by all users.

~~Safeguards Information~~ SGI may be encrypted in two ways. First an individual file can be encrypted with PGP to allow uncontrolled handling and transmission as an email attachment. This will be the method used to forward material to other authorized users. Second, a group of files may be stored in an encrypted volume, "PGPdisk volume," which may be handled as uncontrolled during the period that it is not accessible or "mounted".

Licensee control of encryption software and methods for transmitting SGI must meet the general performance requirements for the protection of ~~safeguards information~~ SGI, found in 10 CFR 73.21. The requirements state that "each licensee... and each person who produces, receives, or acquires Safeguards Information shall ensure that Safeguards Information is protected against unauthorized disclosure." This procedure is intended to supplement existing company procedures for management of SGI material.

3 RESPONSIBILITIES

3.1 Security Manager

3.1.1 Implementation of the SGI encryption program ~~contained~~ described in this procedure.

3.1.2 Ensuring 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 Ensuring individuals have appropriate user level knowledge of PGP software procedures prior to being granted permission to encrypt and electronically transmit SGI.

3.1.4 Granting individual permission to encrypt and transmit ~~Safeguards Information~~ SGI, and maintenance of a list of authorized users. A Sample Authorized User list is provided in attachment 7.1 to this procedure.

3.1.5 Insuring all holders of a public key are promptly notified if ~~part of the key pair is~~ a pass-phrase, keypair, has been, or is suspected of being, compromised.

3.2 Authorized SGI Encryption User (ASEU)

3.2.1 Must have been granted access to ~~Safeguards Information~~ SGI and has an established "need to know" for the information.

3.2.2 Familiar with the company procedures for handling SGI information and the requirements of this procedure for electronic handling, encryption and transmission of SGI.

3.2.3 Familiar with the use of PGP encryption software and has demonstrated the ability to properly use it.

3.2.4 For each public key, maintains a log of all company individuals who have been provided a copy of the public key.

3.2.5 Collects, stores, and handles all company private keys as SGI.

3.2.6 Immediately reports to the Security Manager when a pass-phrase, keypair, or electronic file has been, or is suspected of being, compromised.

4 INSTRUCTIONS

4.1 The following general guidelines should be followed to ensure the proper control of ~~Safeguards Information~~ SGI on computer systems:

4.1.1 No person is allowed access to the unencrypted version of SGI unless the person has an established "need to know" for the information, and has a completed Federal Bureau of Investigation criminal history record information (CHRI) check to the extent required by 10 CFR 73.57.

4.1.2 When in use, the unencrypted SGI must be under the continuous and exclusive control of an individual who is authorized access to the information. The information must be continually attended to by the individual, even though it may not be constantly being used.

4.1.3 SGI may be processed or stored in unencrypted form on computer systems provided that the systems are self-contained stand alone (i.e., laptops designated for SGI, or PCs with a removable hard drives), and not connected to a network with non-safeguards access.

a. While processing unencrypted SGI the computer shall not be left unattended and will be controlled as SGI material.

b. If ~~Safeguards Information~~ SGI is only processed and stored in an encrypted volume (i.e. PGPdisk) the computer may be treated as uncontrolled ~~during periods when the volume is not mounted~~ only after the removable hard drive has been removed and properly stored as SGI material .

1. When the PGP disk is mounted the computer shall be protected as SGI and not connected to a network with non-safeguards access.
2. ~~The computer must have an active antivirus program and provided firewall protection when connected to any network system.~~

c. When a computer that processed SGI is powered down, it may be considered uncontrolled only if all SGI has been processed and stored on a removable hard drive and the hard drive has been removed and properly stored as SGI ~~a determination is made that the memory is free of unencrypted SGI~~. Otherwise the computer must be treated and stored as SGI material.

4.1.4 SGI may only be printed on a stand alone printer~~ and cannot be sent to a printer over a LAN type connection~~.

4.1.5 A computer printer used to print SGI may be 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.

4.2 The following guidelines should be followed for use of PGP encryption software:

4.2.1 Encryption keypair used for SGI:

a. Keypairs shall be generated using a a multi-word passphrase which contains alpha-numeric characters, at least one of which should be a number. The passphrase shall be protected as ~~Safeguards Information~~ SGI.

b. The keypair Full Name shall include the key owner's name and company.

c. The e-mail address listed in the key shall be a company e-mail address that corresponds to the key owner. Private e-mail addresses will not be allowed.

4.2.2 Exchange of public keys:

a. The public key will not be posted to a keyserver.

b. The public key is unprotected.

c. A public key may be provided to an authorized user at another licensee, NEI, and the NRC on electronic media, such as a disk, or ~~by email~~ CD-ROM. Prior to use, the receiving organization must confirm that the key is from an authorized individual. There are two elements, first that the key was provided by the individual listed on the key and second, that the individual is authorized access to ~~safeguards information~~ SGI. ~~This confirmation may be conducted by telephone.~~

d. Each organization shall maintain a list of individuals to whom ~~provided~~ the public key have been provided. These individuals shall be promptly informed if the ~~key is~~ pass-phrase, keypair, has been, or is suspected of being, compromised. Attachment 7.2 provides a sample form.

4.3 Email transmission of encrypted files

4.3.1 A file will be encrypted in a properly protected computer with an SGI removable hard drive or SGI laptop prior to transmission using the appropriate public keys. Conventional Encryption and Self- Decrypting Archives shall not be used.

4.3.2 A ~~transfer~~ memory device, disk, CD, ~~memory stick,~~ etc. is used to ~~move~~ transfer the encrypted file to an unprotected network computer for attachment to an email (usb storage devices are not acceptable for SGI). The unencrypted version of a file shall not be on the memory device used during this transfer process.

4.3.3 Encrypted files may be sent as email attachments to the appropriate addressees. The user should verify that the file is the encrypted version by sighting the addition of the ".pgp" file extension.

4.3.4 Recipients shall move the encrypted email attachment to a properly protected safeguards computer prior to decryption of the file.

4.3.5 Records of electronic transmission of files shall be maintained in the same manner a company maintains records of hard copy material transmission.

4.4 ~~Safeguards Information may be stored in an encrypted volume.~~

~~4.4.1 The volume may be installed on a hard drive, or removable media using PGP disk procedures.~~

~~4.4.2 The PGP disk may be protected by a public key or a pass phrase that contains at least eight alpha-numeric characters.~~

~~4.4.3 When not mounted the volume is uncontrolled. Prior to mounting a volume the computer must meet the criteria for processing safeguards material listed above.~~

~~4.4.4 PGP wipe shall be used when files are deleted from PGPdisk or when removing a PGPdisk prior to release of the device as uncontrolled.~~

5 RECORDS

5.1 The following records will be maintained for review at the station security offices for a period of three years:

5.1.1 Authorized SGI Encryption User (ASEU) List.

5.1.2 Public key distribution list.

6 REFERENCES

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

6.2 10 CFR 73.21 Requirements for the protection of safeguards information.

7 ATTACHMENTS

7.1 Authorized SGI Encryption User (ASEU) List.

7.2 Public key distribution list.