

<NAME>
<TITLE>
<ADDRESS>

SUBJECT:

Dear Mr. or Ms. <NAME>:

By letter dated MM/DD/YYYY, you requested immediate approval for the use of Pretty Good Privacy (PGP) Software (Enterprise, Corporate, or Personal) Desktop Version 8.0.3, the latest validated version developed with PGP Software Development Kit (SDK) 3.0.3 for encryption of sensitive unclassified Safeguards Information (SGI). National Institute of Standards and Technology (NIST) Certificate, Number 394, shows that this software development tool complies with Federal Information Processing Standards 140-2, "Security Requirements for Cryptographic Modules," (FIPS 140-2).

The U.S. Nuclear Regulatory Commission (NRC) staff finds the use of PGP Software Corporate Desktop Version 8.0.3 or newer versions of encryption software is acceptable for processing and transmitting SGI electronically for your site provided that:

1. The PGP software has been developed using a software development tool, PGP SDK 3.0.3, which has been validated by NIST, Certificate, Number 394, to meet FIPS 140-2.
2. NIST-validated Cryptographic Algorithms are used to encrypt data for electronic transmission. These algorithms are listed in the certificate with algorithm certificate numbers. The NIST website, <http://csrc.nist.gov/cryptval/140-1/1401val.htm>, should be checked to ensure that the Cryptographic Algorithms selected for encrypting data are continuously approved by NIST. The NRC approves only those Cryptographic Algorithms approved by NIST. Thus, if NIST no longer approves certain Cryptographic Algorithms, the NRC also does not approve use of that Cryptographic Algorithm.
3. Only one public key is to be generated per site. The PGP file containing the public key must be named according to the following syntax:
LastName_FirstName_SiteName.asc. This naming convention represents the organizational point of contact indicated as owning the key-pair.

Title 10 of the Code of Federal Regulations (10 CFR) Section 73.21(g)(3) states, in part, "... Safeguards Information shall be transmitted only by protected telecommunication circuits (including facsimile) approved by the NRC." The NRC considers those encryption systems that the NIST has determined to be in conformance with the Security Requirements for Cryptographic Modules in Federal Information Processing Standard (FIPS) 140-2, as being acceptable. The Secretary of Commerce has made use of Cryptographic Module Validation Program products mandatory and binding for Federal agencies when a Federal agency determines that cryptography is necessary for protecting sensitive information.

Attachment

Additionally, in accordance with 10 CFR 73.21(a), <LICENSEE NAME> is required to establish and maintain an information protection system that satisfies 10 CFR 73.21(b) through (i). Compliance with the provisions of 10 CFR 73.21, including the use of encryption software for transmittal of SGI, is mandatory and inspectible.

As stated in the letter dated May 5, 2004, from R. P. Zimmerman, NRC, Office of Nuclear Security and Incident Response, to Stephen D. Floyd, Nuclear Energy Institute (NEI), please provide the public key for transmitting sensitive, unclassified SGI and the point of contact information (name, telephone number and e-mail address) to NEI and the NRC points of contact provided below. Once this information has been provided, we will provide a copy of the NRC public key to your point of contact. All SGI holders must employ an appropriate credentialing process to verify that individuals provided with public keys are legitimate users. Private keys must be controlled as SGI.

The NRC technical point of contact regarding the use of PGP is Eric Lee, Security Specialist, Division of Nuclear Security, who can be reached at (301) 415-8099, or via e-mail at exl@nrc.gov. For public key coordination, the NRC point of contact is Mr. Louis Grosman, Office of the Chief Information Officer, who can be contacted at (301) 415-5826, or via e-mail at lhg@nrc.gov. As coordinated with NEI, the industry point of contact for public key coordination is Mr. James W. Davis, who can be reached at (202) 739-8105 or via e-mail at jwd@nei.org.

If you have any questions, please contact me at (301) 415-XXXX.