November 19, 2004

Mr. James W. Davis
Director of Operations
Nuclear Energy Institute
1776 I St. N. W. Suite 400
Washington D.C. 20006

SUBJECT: NUCLEAR ENERGY INSTITUTE USE OF ENCRYPTION SOFTWARE FOR SECURE TRANSMISSION OF SAFEGUARDS INFORMATION

Dear Mr. Davis:

By letter dated October 4, 2004, you requested clarification on whether a May 5, 2004, letter from R. Zimmerman (NRC) to S. Floyd (NEI) authorized the use of Pretty Good Protection (PGP) by NEI and approved the use of PGP Software (Enterprise, Corporate, or Personal) Desktop Version 8.0.3 developed with PGP Software Development Kit (SDK) 3.0.3 for encryption of sensitive unclassified SGI. Based on the discussion below, the NRC authorizes NEI to use PGP to transmit safeguards information (SGI) to authorized SGI holders and approves the use of PGP software developed using PGP SDK 3.0.3, or any other cryptographic modules approved by National Institute of Standards and Technology (NIST), which are posted on the NIST website (http://csrc.nist.gov/cryptval/140-1/1401val.htm). Specifically, the Federal Information Processing Standards approved cryptographic algorithms using the above software are acceptable.

Title 10 of the Code of Federal Regulations (10 CFR) Section 73.21(g)(3) states in part that "... Safeguards Information shall be transmitted only by protected telecommunication circuits (including facsimile) approved by the NRC." The NRC considers those encryption systems that NIST has determined conform to the Security Requirements for Cryptographic Modules in Federal Information Processing Standard (FIPS) 140-2 as being acceptable.

Authorized SGI holders who wish to employ electronic data encryption for the transmission of safeguards information (SGI) should submit a written request for NRC approval consistent with the guidance in RIS 2002-15. Although you have not submitted such a written request for NRC approval, taking consideration of (1) your February 23, 2004, and March 26, 2004, letters, and (2) your effort to coordinate and manage the collection and distribution of public keys among interested SGI holders within the nuclear power industry, pursuant to your your October 18, 2004 telephone request, your October 4, 2004, letter will be treated as a written request for NRC approval to use data encryption for the transmission of SGI.

NRC's approval of your request to use data encryption software to transmit SGI is contingent upon you and your communication partners (licensees) continuing to be in compliance with the provisions of 10 CFR 73.21, "Requirements for the Protection of Safeguards Information." In accordance with 10 CFR 73.21(a), authorized SGI holders are required to establish and maintain an information protection system that satisfies 10 CFR 73.21(b) through (i). Use of NIST-approved data encryption software in conjunction with an information protection system that satisfies 10 CFR 73.21(b) through (i) constitutes a protected communications circuit pursuant to 10 CFR 73.21(g)(3). Compliance with the provisions of 10 CFR 73.21 is subject to inspection by the NRC staff.

The procedure developed by NEI on the use of encryption software for management and transmission of SGI is acceptable with modifications (Please refer to the enclosure of our May 5, 2004, letter). This modified procedure may be adopted by authorized SGI holders as an acceptable, standardized process for the encryption and exchange of SGI among authorized SGI holders, and between authorized SGI holders and the NRC.

As you have indicated, PGP Software Corporate Desktop Version 8.0.3 was developed with PGP SDK 3.0.3. NIST Certificate Number 394 validates compliance of this software development tool with FIPS 140-2 requirements. Thus, PGP Software Corporate Desktop Version 8.0.3 software is acceptable for processing and transmitting SGI electronically for your company. Other encryption software or later version of PGP Software Corporate Desktop are also acceptable provided that:

1. Encryption software is developed using NIST approved cryptographic modules (i.e., PGP SDK 3.0.3, NIST Certificate, Number 394).

2. You notify the NRC of your intention to update your encryption software 30 days prior to its first use. When notifying the NRC, include a description of the new software you will be using and provide a statement indicating NIST certification of the software development tool.

If you have any questions, please contact me at (301)415-7083.

Sincerely,

/RA/ SM

Scott Morris, Chief
Reactor Security Section
Division of Nuclear Security
Office of Nuclear Security Incident Response

The procedure developed by NEI on the use of encryption software for management and transmission of SGI is acceptable with modifications (See the enclosure of the May 5, 2004, letter (ML041180613). This modified procedure may be adopted by authorized SGI holders as an acceptable, standardized process for the encryption and exchange of SGI among authorized SGI holders, and between authorized SGI holders and the NRC.

As you have indicated, PGP Software Corporate Desktop Version 8.0.3 was developed with PGP SDK 3.0.3. NIST Certificate Number 394 validates compliance of this software development tool with FIPS 140-2 requirements. Thus, PGP Software Corporate Desktop Version 8.0.3 software is acceptable for processing and transmitting SGI electronically for your company. Other encryption software or later version of PGP Software Corporate Desktop are also acceptable provided that:

3. Encryption software is developed using NIST approved cryptographic modules (i.e., PGP SDK 3.0.3, NIST Certificate, Number 394).

4. You notify the NRC of your intention to update your encryption software 30 days prior to its first use. When notifying the NRC, include a description of the new software you will be using and provide a statement indicating NIST certification of the software development tool.

If you have any questions, please contact me at (301)415-7083.

Sincerely,

/RA/ SM

Scott Morris, Chief
Reactor Security Section
Division of Nuclear Security
Office of Nuclear Security Incident Response

DISTRIBUTION: (Electronic)
RidsNsirOd
DNS r/f
ACCESSION NO.: ML043170378 TEMPLATE NO.: NSIR-002
* See Previous Concurrence
9 Non-Public K Public 9 Sensitive K Non-Sensitive

OFFICE	DNS/NSIR	SC:DNS/NSIR	D:DNS/NSIR
NAME	E Lee*	S Morris*	S. Morris /f/Shea*
DATE	11/19 /04	11/19 /04	11/19 /04

OFFICIAL RECORD ONLY