Nebraska Public Power District
Always there when you need us

NLS2004073

May 28, 2004

U. S. Nuclear Regulatory Commission
Attention: Document Control Desk
Washington, DC 20555-0001

References:
1. 10 CFR 73.21
2. Nuclear Regulatory Commission (NRC) Regulatory Issue Summary 2002-15

Subject: Use of Encryption Software for Electronic Transmission of Safeguards Information, Cooper Nuclear Station, Docket No. 50-298, License No. DPR-46

The purpose of this letter is to request approval for Nebraska Public Power District (NPPD) to process and transmit Safeguards Information (SGI) using PGP Software Corporate Desktop Version 8.0 or the latest validated version, developed with PGP Software Development Kit (SDK) 3.0.3, pursuant to the requirements of 10 CFR 73.21(g)(3). The 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.

NPPD intends to exchange SGI with the NRC, Nuclear Energy Institute (NEI), and other SGI holders who have received NRC approval to use PGP software. Mr. Marty Faulkner, Security Manager, is responsible for the overall implementation of the SGI encryption program at NPPD. Mr. Patrick Carlock, Security Operations Supervisor, is responsible for collecting, safeguarding, and dissemination the software tools needed for encryption and disseminating the software tools needed for encryption and decryption of SGI.

5008

COOPER NUCLEAR STATION
P.O. Box 98 / Brownville, NE 68321-0098
***Telephone:** (402) 825-3811 / **Fax:** (402) 825-5211*
www.nppd.com

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).

Should you have any questions or require additional information, please contact Mr. Paul Fleming, Licensing Manager at 402-825-2774.

Randall K. Edington
Vice President-Nuclear and
Chief Nuclear Officer

/nr

cc: Regional Administrator
USNRC - Region IV

Senior Project Manager
USNRC - NRR Project Directorate IV-1

Senior Resident Inspector
USNRC

NPG Distribution

CNS Records

Scott Morris
USNRC, Office of Nuclear Security and Incident Response,
Reactor Security Section

Lynn Silvious
USNRC, Office of Nuclear Security and Incident Response,
Information Security Section

Louis Grosman
USNRC, Office of the Chief Information Officer

James Davis, Nuclear Energy Institute

Correspondence Number: NLS2004073

The following table identifies those actions committed to by Nebraska Public Power District (NPPD) in this document. Any other actions discussed in the submittal represent intended or planned actions by NPPD. They are described for information only and are not regulatory commitments. Please notify the Licensing & Regulatory Affairs Manager at Cooper Nuclear Station of any questions regarding this document or any associated regulatory commitments.

COMMITMENT	COMMITTED DATE OR OUTAGE
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.	Prior to first use for SGI material.