FENOC
FirstEnergy Nuclear Operating Company

Beaver Valley Power Station
Route 168
P.O. Box 4
Shippingport, PA 15077-0004

L. William Pearce
Site Vice President

724-682-5234
Fax: 724-643-8069

June 1, 2004
L-04-069

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

Subject: Beaver Valley Power Station, Unit No. 1 and No. 2
BV-1 Docket No. 50-334, License No. DPR-66
BV-2 Docket No. 50-412, License No. NPF-73
Use of Encryption Software for Electronic Transmission of Safeguards Information

Pursuant to the requirements of 10 CFR 73.21(g)(3), FirstEnergy Nuclear Operating Company (FENOC) requests approval to process and transmit Safeguards Information (SGI) at the Beaver Valley Power Station (BVPS) 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.

FENOC 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. Richard W. Dibler, Access Authorization Supervisor is responsible for the overall implementation of the SGI encryption program at BVPS. Mr. Gary L. Garrett, FENOC IT Transition Manager – Business Unit Support is responsible for collecting, safeguarding, and disseminating the software tools needed for encryption and decryption of SGI for FENOC.

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. Kenneth E. Halliday, Manager, Nuclear Security at 724-682-5072.

Sincerely,

L. William Pearce

References:

10 CFR 73.21
NRC Regulatory Issue Summary 2002-15

Attachments:

A. List of Regulatory Commitments

c: Mr. T. G. Colburn, NRR Senior Project Manager
Mr. P. C. Cataldo, NRC Sr. Resident Inspector
Mr. H. J. Miller, NRC Region I Administrator
Mr. Scott Morris, NRC/NISR
Mr. Lynn Silvious, NRC/NSIR
Mr. Louis Grosman, NRC/OCIO
Mr. James Davis, NEI

ATTACHMENT A

Commitment List

The following list identifies those actions committed to by FirstEnergy Nuclear Operating Company (FENOC) for Beaver Valley Power Station (BVPS) Unit Nos. 1 and 2 in this document. Any other actions discussed in the submittal represent intended or planned actions by Beaver Valley. These other actions are described only as information and are not regulatory commitments. Please notify Mr. Larry R. Freeland, Manager, Regulatory Affairs/Performance Improvement, at Beaver Valley on (724) 682-5284 of any questions regarding this document or associated regulatory commitments.

Commitment	Due Date
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 the first use of encryption software for SGI material.