UNITED STATES
NUCLEAR REGULATORY COMMISSION
WASHINGTON, D.C. 20555-0001

December 6, 2005

Mr. T. A. Sullivan
Site Vice President, JAF
Entergy Nuclear Operations, Inc.
James A. Fitzpatrick NPP
P.O. Box 110
Lycoming, NY 13093

SUBJECT: USE OF PRIVATEL TELEPHONE SECURITY DEVICES FOR ELECTRONIC TRANSMISSION OF SAFEGUARDS INFORMATION

Dear Mr. Sullivan:

By letter dated September 26, 2005, you requested immediate approval for the use of Privatel model 960V, software version 7.10 telephone devices for the purpose of establishing protected telecommunications and transmitting encoded Safeguards Information (SGI) between authorized individuals over these protected telecommunication devices. National Institute of Standards and Technology (NIST) Certificate, Number 108, shows that Privatel model 960V, software version 7.10 telephone device complies with Federal Information Processing Standards 140-1, "Security Requirements for Cryptographic Modules" (FIPS 140-1).

The U.S. Nuclear Regulatory Commission (NRC) staff finds the use of Privatel model 960V, software version 7.10 telephone is acceptable for processing and transmitting SGI electronically for your site provided that 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.

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.

Additionally, in accordance with 10 CFR 73.21(a), the licensee 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 media for voice communications involving SGI, is mandatory and inspectible.

The NRC technical point of contact regarding the use of encryption devices 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.

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

Sincerely

/RA/

Scott A. Morris, Chief
Reactor Security Section
Division of Nuclear Security
Office Of Nuclear Security and Incident Response

The NRC technical point of contact regarding the use of encryption devices 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. .

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

Sincerely

(Original Signed by:)

Scott A. Morris, Chief
Reactor Security Section
Division of Nuclear Security
Office Of Nuclear Security and Incident Response

DISTRIBUTION: (Electronic)
DNS R/F B. Stapleton

TEMPLATE NO.: NSIR-002
ACCESSION NO.: ML053210139 *see previous concurrence

OFFICE	DNS/NSIR	SC:DNS/NSIR	NRR/LPLI-1
NAME	ELee*	SMorris*	JPBoska
DATE	11/30/05	12/05/05	12/06/05