August 3, 2011

Mr. Jay P. Fischer
Trojan ISFSI Manager
Portland General Electric Company
71760 Columbia River Hwy
Rainier, Oregon 97048

SUBJECT: USE OF ENCRYPTION SOFTWARE FOR ELECTRONIC TRANSMISSION OF SAFEGUARDS INFORMATION

Dear Mr. Fischer:

By letter dated July 7, 2011, Portland General Electric Company requested approval for the use of Pretty Good Privacy (PGP) Desktop Email, developed with PGP Software Developer's Kit (SDK) for encryption of sensitive unclassified Safeguards Information (SGI). National Institute of Standards and Technology (NIST) Certificate (Number 1101) 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 Desktop Email 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 4.0.1, which has been validated by NIST, Certificate Number 1101 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/groups/STM/cmvp/documents/140-1/140val-all.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. Addressees may replace the current version of encryption products that were approved by the NRC with a newer version of encryption product without prior approval from the NRC, provided that the addressees document that the newer version of encryption product, i.e., document that the FIPS validation certificate of the newer version of encryption product is the same as the current version of encryption product.

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 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.

The public key should be named according to the following syntax: LastName_FirstName_Organization.asc. This naming convention represents the organizational point of contact indicated as owning the key. Please provide the public key for transmitting sensitive, unclassified SGI and the point of contact information (name, telephone number and e-mail address) to the NRC point of contact provided below. 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 Monika Coflin, Cyber Security Specialist, Division of Security Policy, who can be reached at (301)415-6659 or via e-mail at monika.coflin@nrc.gov.

If you have any questions, please contact me at (301) 415-5374.

Sincerely,

/RA/

Craig G. Erlanger, Chief
Cyber Security and Integrated Response Branch
Division of Security Policy
Office of Nuclear Security and Incident Response

(including facsimile) approved by the NRC." 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.

The public key should be named according to the following syntax: LastName_FirstName_Organization.asc. This naming convention represents the organizational point of contact indicated as owning the key. Please provide the public key for transmitting sensitive, unclassified SGI and the point of contact information (name, telephone number and e-mail address) to the NRC point of contact provided below. 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 Monika Coflin, Cyber Security Specialist, Division of Security Policy, who can be reached at (301)415-6659 or via e-mail at monika.coflin@nrc.gov.

If you have any questions, please contact me at (301) 415-5374.

Sincerely,

/RA/

Craig G. Erlanger, Chief
Cyber Security and Integrated Response Branch
Division of Security Policy
Office of Nuclear Security and Incident Response

DISTRIBUTION:
DSP r/f

ADAMS Accession number: ML112000359

OFFICE	NSIR/DSP	NSIR/DSP	NSIR/DSO	NSIR/DSP
NAME	MCoflin	SWastler	BStapleton	CErlanger
DATE	7/21/11	07/28/11	08/01/2011	08/03/2011

OFFICIAL RECORD COPY