



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

December 6, 2016

Mr. Joseph W. Shea
Vice President, Nuclear Licensing
Tennessee Valley Authority
1101 Market Street, LP 3R-C
Chattanooga, TN 37402-2801

SUBJECT: BROWNS FERRY NUCLEAR PLANT, UNITS 1, 2, AND 3; SEQUOYAH
NUCLEAR PLANT, UNITS 1 AND 2; WATTS BAR NUCLEAR PLANT, UNITS 1
AND 2 – USE OF ENCRYPTION SOFTWARE FOR ELECTRONIC
TRANSMISSION OF SAFEGUARDS INFORMATION (CAC NOS. MF8704,
MF8705, MF8706, MF8707, MF8708, MF8709, AND MF8710)

Dear Mr. Shea:

By letter dated October 28, 2016 (Agencywide Documents Access and Management System (ADAMS) Accession No. ML16302A438), Tennessee Valley Authority (TVA) requested the U.S. Nuclear Regulatory Commission (NRC) approval to use Symantec Endpoint Encryption by PGP Technology, 11.1, or the latest validated version, to process and transmit safeguards information (SGI) in accordance with Title 10 of the *Code of Federal Regulations* (10 CFR) Paragraph 73.22(f)(3).

Section 73.22(f) of 10 CFR, "External transmission of documents and material," describes requirements for the transmission of SGI outside an authorized place of use or storage. Paragraph 73.22(f)(3) of 10 CFR states, in part:

Except under emergency or extraordinary conditions, Safeguards Information shall be transmitted outside an authorized place of use or storage only by NRC approved secure electronic devices, such as facsimiles or telephone devices, provided that transmitters and receivers implement processes that will provide high assurance that Safeguards Information is protected before and after the transmission or electronic mail through the internet, provided that the information is encrypted by a method (Federal Information Processing Standard [FIPS] 140-2 or later) approved by the appropriate NRC Office; the information is produced by a self contained secure automatic data process system; and transmitters and receivers implement the information handling processes that will provide high assurance that Safeguards Information is protected before and after transmission.

Guidance to licensees on the electronic transmission of Safeguards Information is provided in NRC Regulatory Issue Summary 2002-15, Revision 1, "NRC Approval of Commercial Data Encryption Products for the Electronic Transmission of Safeguards Information," dated January 26, 2006 (ADAMS) Accession No. ML050460031).

As stated in TVA's letter, Symantec Endpoint Encryption by PGP Technology, 11.1 was developed with PGP Cryptographic Engine Software Version 4.3 and complies with FIPS 140-2 as validated by the National Institute of Standards and Technology (NIST) Consolidated Certificate No. 0053. A copy of the certificate was enclosed with TVA's letter.

The NRC approves only those cryptographic algorithms approved by NIST. Based on the NIST validation that the encryption software complies with FIPS 140-2, the NRC staff finds that the use of Symantec Endpoint Encryption by PGP Technology, 11.1 is acceptable to use for electronic transmission of SGI in accordance with 10 CFR 73.22(f)(3). As described in RIS-2002-15, newer versions of this software may be used, without prior NRC approval, provided there's documentation that the newer version uses the same cryptographic module as the current version. Thus, the staff approves the use of Symantec Endpoint Encryption by PGP Technology, 11.1 in accordance with 10 CFR 73.22(f)(3), at all of TVA's NRC-licensed facilities. If NIST no longer approves certain cryptographic algorithms, the NRC also does not approve use of that cryptographic algorithm.

If you have any questions, please contact me at 301-415-1383.

Sincerely,



Perry H. Buckberg, Senior Project Manager
Plant Licensing II-2
Division of Operating Reactor Licensing
Office of Nuclear Reactor Regulation

Docket Nos. 50-259, 50-260, 50-296,
50-327, 50-328, 50-390, 50-391

cc: Distribution via Listserv

J. Shea

- 2 -

As stated in TVA's letter, Symantec Endpoint Encryption by PGP Technology, 11.1 was developed with PGP Cryptographic Engine Software Version 4.3 and complies with FIPS 140-2 as validated by the National Institute of Standards and Technology (NIST) Consolidated Certificate No. 0053. A copy of the certificate was enclosed with TVA's letter.

The NRC approves only those cryptographic algorithms approved by NIST. Based on the NIST validation that the encryption software complies with FIPS 140-2, the NRC staff finds that the use of Symantec Endpoint Encryption by PGP Technology, 11.1 is acceptable to use for electronic transmission of SGI in accordance with 10 CFR 73.22(f)(3). As described in RIS-2002-15, newer versions of this software may be used, without prior NRC approval, provided there's documentation that the newer version uses the same cryptographic module as the current version. Thus, the staff approves the use of Symantec Endpoint Encryption by PGP Technology, 11.1 in accordance with 10 CFR 73.22(f)(3), at all of TVA's NRC-licensed facilities. If NIST no longer approves certain cryptographic algorithms, the NRC also does not approve use of that cryptographic algorithm.

If you have any questions, please contact me at 301-415-1383.

Sincerely,

/RA/

Perry H. Buckberg, Senior Project Manager
Plant Licensing II-2
Division of Operating Reactor Licensing
Office of Nuclear Reactor Regulation

Docket Nos. 50-259, 50-260, 50-296,
50-327, 50-328, 50-390, 50-391

cc: Distribution via Listserv

DISTRIBUTION:

PUBLIC LPL2-2 R/F
RidsNrrLABClayton Resource
RidsAcrr_MailCTR Resource

RidsNrrDorLpl2-2 Resource
RidsNrrPMWattsBar Resource
RidsNrrPMBrownsferry Resource

RidsNrrPMSequoyah Resource
DParsons, NSIR

ADAMS Accession No. ML16313A281

***by e-mail**

OFFICE	NRR/LPL2-2/PM	NRR/LPL2-2/LA	NSIR/DSO/ISB/BC*	OGC*
NAME	PBuckberg	BClayton	DParsons (RNorman for)	JBielecki
DATE	12/01/16	12/06/16	12/01/16	12/01/16
OFFICE	NRR/LPL2-2/BC(A)	NRR/LPL2-2/PM		
NAME	JDion	PBuckberg		
DATE	12/05/16	12/06/16		

OFFICIAL RECORD COPY