Tennessee Valley Authority, 1101 Market Street, Chattanooga, Tennessee 37402

CNL-16-144

October 28, 2016

10 CFR 73.22

ATTN: Document Control Desk
U.S. Nuclear Regulatory Commission
Washington, D.C. 20555-0001

Browns Ferry Nuclear Plant, Units 1, 2, and 3
Renewed Facility Operating License Nos. DPR-33, DPR-52, and DPR-68
NRC Docket Nos. 50-259, 50-260, and 50-296

Sequoyah Nuclear Plant, Units 1 and 2
Renewed Facility Operating License Nos. DPR-77 and DPR-79
NRC Docket Nos. 50-327 and 50-328

Watts Bar Nuclear Plant, Units 1 and 2
Facility Operating License Nos. NPF-90 and NPF-96
NRC Docket No. 50-390 and 50-391

Subject: **Use of Encryption Software for Electronic Transmission of Safeguards Information**

References:
1. NRC Regulatory Guide 5.79, "Protection of Safeguards Information," April 2011
2. NRC Regulatory Issue Summary 2002-15, Revision 1, "NRC Approval of Commercial Data Encryption Systems for the Electronic Transmission of Safeguards Information," dated January 26, 2006

Pursuant to the requirements of Title 10 of the *Code of Federal Regulations* (10CFR) 73.22(f)(3) and the guidance provided in Nuclear Regulatory Commission (NRC) Regulatory Guide 5.79 (Reference 1) and Regulatory Issue Summary 2002-15, Revision 1 (Reference 2), Tennessee Valley Authority (TVA) requests approval to process and transmit safeguards information (SGI) using Symantec Endpoint Encryption by PGP Technology, 11.1, or the latest validated version. This version of encryption product was developed with PGP Cryptographic Engine Software Version 4.3 and complies with Federal Information Processing Standard (FIPS) 140-2 as validated by the National Institute of Standards and Technology (NIST) Consolidated Certificate No. 0053 (Enclosure).

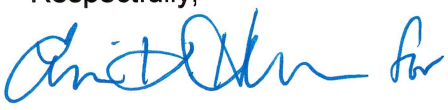
TVA has and continues to maintain an established written procedure in place that describes, as a minimum: access controls; where and when encrypted communications can be made; how encryption keys, codes and passwords are protected from compromise; actions to be taken if the encryption keys, codes or passwords are, or are suspected to have been, compromised (such as notification of all authorized users); and how the identity and access authorization of the recipient will be verified.

TVA intends to exchange SGI with the NRC, Nuclear Energy Institute, and other SGI holders who have received NRC approval to use PGP software. Pursuant to 10 CFR 73.22(f)(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 73.22(g).

Patrick J. Asendorf, Senior Program Manager, Security Regulatory Oversight, is responsible for the overall implementation of the SGI encryption program at TVA. Mr. Asendorf is also responsible for collecting, safeguarding and disseminating the software tools needed for encryption and decryption of SGI.

There are no new regulatory commitments contained in this submittal. If you have any questions concerning this matter, please contact Patrick J. Asendorf at (423) 751-8150.

Respectfully,



J. W. Shea
Vice President, Nuclear Licensing

Enclosure: FIPS 140-2 Consolidated Certificate No. 0053

cc (Enclosure):

NRC Regional Administrator – Region II
NRC Senior Resident Inspector – Browns Ferry Nuclear Plant
NRC Senior Resident Inspector – Sequoyah Nuclear Plant
NRC Senior Resident Inspector – Watts Bar Nuclear Plant
NRC Project Manager – Browns Ferry Nuclear Plant
NRC Project Manager – Sequoyah Nuclear Plant
NRC Project Manager – Watts Bar Nuclear Plant

ENCLOSURE

FIPS 140-2 Consolidated Certificate No. 0053

FIPS 140-2 Consolidated Validation Certificate

The National Institute of Standards and Technology of the United States of America

The Communications Security Establishment of the Government of Canada

Consolidated Certificate No. 0053

The National Institute of Standards and Technology, as the United States FIPS 140-2 Cryptographic Module Validation Authority; and the Communications Security Establishment Canada, as the Canadian FIPS 140-2 Cryptographic Module Validation Authority; hereby validate the FIPS 140-2 testing results of the cryptographic modules listed below in accordance with the Derived Test Requirements for FIPS 140-2, Security Requirements for Cryptographic Modules. FIPS 140-2 specifies the security requirements that are to be satisfied by a cryptographic module utilized within a security system protecting Sensitive Information (United States) or Protected Information (Canada) within computer and telecommunications systems (including voice systems).

Products which use a cryptographic module identified below may be labeled as complying with the requirements of FIPS 140-2 so long as the product, throughout its life-cycle, continues to use the validated version of the cryptographic module as specified in this consolidated certificate. The validation report contains additional details concerning test results. No reliability test has been performed and no warranty of the products by both agencies is either expressed or implied.

FIPS 140-2 provides four increasing, qualitative levels of security: Level 1, Level 2, Level 3, and Level 4. These levels are intended to cover the wide range and potential applications and environments in which cryptographic modules may be employed. The security requirements cover eleven areas related to the secure design and implementation of a cryptographic module.

The scope of conformance achieved by the cryptographic modules as tested are identified and listed on the Cryptographic Module Validation Program website. The website listing is the official list of validated cryptographic modules. Each validation entry corresponds to a uniquely assigned certificate number. Associated with each certificate number is the module name(s), module versioning information, applicable caveats, module type, date of initial validation and applicable revisions, Overall Level, individual Levels if different than the Overall Level, FIPS-approved and other algorithms, vendor contact information, a vendor provided description and the accredited Cryptographic Module Testing laboratory which performed the testing.

Signed on behalf of the Government of the United States

Signature: Michael J Cooper

Dated: 5 June 2015

Chief, Computer Security Division
National Institute of Standards and Technology

Signed on behalf of the Government of Canada

Signature:

Dated: 5 June 2015

Director, Architecture and Technology Assurance
Communications Security Establishment Canada

TM: A Certification Mark of NIST, which does not imply product endorsement by NIST the U.S. or Canadian Governments

Certificate Number	Validation / Posting Date	Module Name(s)	Vendor Name	Version Information
2356	05/19/2015	Kernel Mode Cryptographic Primitives Library (cng.sys) in Microsoft Windows 8.1 Enterprise, Windows Server 2012 R2, Windows Storage Server 2012 R2, Surface Pro 3, Surface Pro 2, Surface Pro, Surface 2, Surface, Windows RT 8.1, Windows Phone 8.1, Windows Embedded 8.1 Industry Enterprise, StorSimple 8000 Series	Microsoft Corporation	Software Versions: 6.3.9600 and 6.3.9600.17042
2365	5/4/2015	Cisco Systems 5508 Wireless LAN Controller	Cisco Systems, Inc.	Hardware Version: 5508 with 5508 FIPS kit (AIR-CT5508FIPSKIT=) and CN56XX; Firmware Version: 8.0 with SNMP Stack v15.3, OPENSSL-0.9.8g-8.0.0, QUICKSEC-2.0-8.0 and FP-CRYPTO-7.0.0
2366	5/4/2015	FortiGate-60C/60D/80C and FortiWiFi-60C/60D	Fortinet, Inc.	Hardware Versions: C4DM93 [1], C1AB28 [2], C4BC61[3], C4DM95 [4], and C1AB32 [5] with Tamper Evident Seal Kits: FIPS-SEAL-BLUE [3] or FIPS-SEAL-RED [1,2,4,5]; Firmware Version: 5.0, build0305, 141216
2367	5/4/2015	FortiGate-100D, FortiGate-200B, FortiGate-200D, FortiGate-300C, FortiGate-600C and FortiGate-800C	Fortinet, Inc.	Hardware Versions: C4LL40 [1], C4CD24 [2], C4KV72 [3], C4HY50 [4], C4HZ51 [5] and C4LH81 [6] with Tamper Evident Seal Kits: FIPS-SEAL-BLUE [2] or FIPS-SEAL-RED [1,3,4,5,6]; Firmware Version: 5.0, build0305,141216
2368	5/4/2015	FortiGate-1000C, FortiGate-1240B, FortiGate-3140B and FortiGate-3240C	Fortinet, Inc.	Hardware Versions: C4HR40 [1], C4CN43 [2], C4XC55 [3] and C4KC75 [4] with Tamper Evident Seal Kits: FIPS-SEAL-RED [1,3,4] or FIPS-SEAL-BLUE [2]; Firmware Version: FortiOS 5.0, build0305,141216

Certificate Number	Validation / Posting Date	Module Name(s)	Vendor Name	Version Information
2369	5/4/2015	FortiGate-1500D and 3700D	Fortinet, Inc.	Hardware Versions: C1AA64 [1] and C1AA92 [2] with Tamper Evident Seal Kits: FIPS-SEAL-RED [1,2]; Firmware Version: FortiOS 5.0, build0305,141216
2370	5/4/2015	FortiOS™ 5.0	Fortinet, Inc.	Firmware Version: 5.0, build0305, 141216
2371	5/4/2015	FortiGate-3600C and FortiGate-3950B	Fortinet, Inc.	Hardware Versions: C4MH12, [C4DE23 with P06698-02] with Tamper Evident Seal Kits: FIPS-SEAL-RED; Firmware Version: FortiOS 5.0, build0305,141216
2372	05/05/2015	FortiGate-5140B Chassis with FortiGate/FortiSwitch 5000 Series Blades	Fortinet, Inc.	Hardware Version: Chassis: P09297-01; Blades: P4CJ36-04, P4EV74, C4LG17 and P4EX84; AMC Component: P4FC12; Air Filter: PN P10938-01; Front Filler Panel: PN P10945-01: ten; Rear Filler Panel: PN P10946-01: fourteen; Tamper Evident Seal Kit: FIPS-SEAL-RED; Firmware Version: FortiOS 5.0, build0305, 141216
2373	05/05/2015	Neopost Postal Security Device (PSD)	Neopost Technologies, S.A.	Hardware Version: A0014227-B; Firmware Version: a30.00; P/N: A0038091-A
2374	05/08/2015	Avaya WLAN 9100 Access Points	Avaya Inc.	Hardware Versions: P/Ns WAO912200-E6GS [1], WAP913200-E6GS [2], WAP913300-E6GS [2], WAP917300-E6GS [2]; Enclosure (Form Factor): WAO912200-E6GS [1], WAB910003-E6 [2]; SKU WLB910001-E6; Firmware Version: AOS-7.1
2375	05/20/2015	HP P-Class Smart Array RAID Controllers	Hewlett-Packard Development Company, L.P.	Hardware Versions: P230i, P430, P431, P731m, P830, and P830i; Firmware Version: 1.66

Certificate Number	Validation / Posting Date	Module Name(s)	Vendor Name	Version Information
2376	05/21/2015	Aegis Secure Key 3.0 Cryptographic Module	Apricorn Inc.	Hardware Version: RevD; Firmware Version: 6.5
2377	5/21/2015	Symantec PGP Cryptographic Engine	Symantec Corporation	Software Version: 4.3
2379	05/21/2015	Ciena 6500 Packet-Optical Platform 4x10G	Ciena Corporation	Hardware Version: 1.0; Firmware Version: 1.10
2380	05/21/2015	Samsung UFS (Universal Flash Storage) Shark SED	Samsung Electronics Co., Ltd.	Hardware Versions: KLUAG2G1BD-B0B2, KLUBG4G1BD-B0B1, KLUCG8G1BD-B0B1; Firmware Version: 0102

Certificate Number	Validation / Posting Date	Module Name(s)	Vendor Name	Version Information
2381	05/21/2015	Brocade® MLXe®, Brocade® NetIron® CER 2000 Ethernet Routers and Brocade CES 2000 Routers and Switches	Brocade Communications Systems, Inc.	Hardware Versions: {[BR-MLXE-4-MR-M-AC (P/N: 80-1006853-01), BR-MLXE-4-MR-M-DC (P/N: 80-1006854-01), BR-MLXE-8-MR-M-AC (P/N: 80-1004809-04), BR-MLXE-8-MR-M-DC (P/N: 80-1004811-04), BR-MLXE-16-MR-M-AC (P/N: 80-1006820-02), BR-MLXE-16-MR-M-DC (P/N: 80-1006822-02), BR-MLXE-4-MR2-M-AC (P/N: 80-1006870-01), BR-MLXE-4-MR2-M-DC (P/N: 80-1006872-01), BR-MLXE-8-MR2-M-AC (P/N: 80-1007225-01), BR-MLXE-8-MR2-M-DC (P/N: 80-1007226-01), BR-MLXE-16-MR2-M-AC (P/N: 80-1006827-02), BR-MLXE-16-MR2-M-DC (P/N: 80-1006828-02)] with Component P/Ns 80-1006778-01, 80-1005643-01, 80-1003891-02, 80-1002983-01,80-1003971-01,80-1003972-01, 80-1003811-02, 80-1002756-03, 80-1004114-01,80-1004113-01,80-1004112-01, 80-1004760-02, 80-1006511-02, 80-1004757-02, 80-1003009-01, 80-1003052-01, 80-1003053-01, NI-CER-2048F-ADVPREM-AC (P/N: 80-1003769-07), NI-CER-2048F-ADVPREM-DC (P/N: 80-1003770-08), NI-CER-2048FX-ADVPREM-AC (P/N: 80-1003771-07), NI-CER-2048FX-ADVPREM-DC (P/N: 80-1003772-08), NI-CER-2024F-ADVPREM-AC (P/N: 80-1006902-02), NI-CER-2024F-ADVPREM-DC (P/N: 80-1006904-02), NI-CER-2024C-ADVPREM-AC (P/N: 80-1007032-02), NI-CER-2024C-ADVPREM-DC (P/N: 80-1007034-02), NI-CER-2048C-ADVPREM-AC (P/N: 80-

Certificate Number	Validation / Posting Date	Module Name(s)	Vendor Name	Version Information
				1007039-02), NI-CER-2048C-ADVPREM-DC (P/N: 80-1007040-02), NI-CER-2048CX-ADVPREM-AC (P/N: 80-1007041-02), NI-CER-2048CX-ADVPREM-DC (P/N: 80-1007042-02), BR-CER-2024F-4X-RT-DC (P/N: 80-1007212-01), BR-CER-2024C-4X-RT-DC (P/N: 80-1007213-01), BR-CER-2024F-4X-RT-AC (P/N: 80-1006529-01), BR-CER-2024C-4X-RT-AC (P/N: 80-1006530-01), NI-CER-2024C-2X10G (P/N: 80-1003719-03), BR-CES-2024C-4X-AC (P/N: 80-1000077-01), BR-CES-2024C-4X-DC (P/N: 80-1007215-01), BR-CES-2024F-4X-AC (P/N: 80-1000037-01), BR-CES-2024F-4X-DC (P/N: 80-1007214-01), RPS9 (P/N: 80-1003868-01) and RPS9DC (P/N: 80-1003869-02)} with FIPS Kit XBR-000195; Firmware Version: Multi-Service IronWare R05.7.00
2382	05/21/2015	HGST Ultrastar 7K6000 TCG Enterprise HDDs	HGST, Inc.	Hardware Versions: P/Ns HUS726060AL5215 (0001); HUS726060AL4215 (0001); HUS726050AL5215 (0001); HUS726050AL4215 (0001); HUS726040AL5215 (0001); HUS726040AL4215 (0001); HUS726030AL5215 (0001); HUS726030AL4215 (0001); HUS726020AL5215 (0001); HUS726020AL4215 (0001); Firmware Version: R519
2383	05/21/2015	HP Virtual Connect 16Gb 24-Port FC Module	Hewlett-Packard Company	Hardware Version: 40-1000779-08 Rev C (80-1007799-04); Firmware Version: VC 4.40

Certificate Number	Validation / Posting Date	Module Name(s)	Vendor Name	Version Information
2384	05/21/2015	Brocade® DCX, DCX 8510-8, DCX-4S and DCX 8510-4 Backbones, 6510 FC Switch, 6520 FC Switch and 7800 Extension Switch	Brocade Communications Systems, Inc.	Hardware Versions: {[DCX Backbone (P/Ns 80-1001064-10, 80-1006751-01, 80-1004920-04 and 80-1006752-01), DCX-4S Backbone (P/Ns 80-1002071-10, 80-1006773-01, 80-1002066-10 and 80-1006772-01), DCX 8510-4 Backbone (P/Ns 80-1004697-04, 80-1006963-01, 80-1005158-04 and 80-1006964-01), DCX 8510-8 Backbone (P/Ns 80-1004917-04 and 80-1007025-01)] with Blades (P/Ns 80-1001070-07, 80-1006794-01, 80-1004897-01, 80-1004898-01, 80-1002000-02, 80-1006771-01, 80-1001071-02, 80-1006750-01, 80-1005166-02, 80-1005187-02, 80-1001066-01, 80-1006936-01, 80-1001067-01, 80-1006779-01, 80-1001453-01, 80-1006823-01, 80-1003887-01, 80-1007000-01, 80-1002839-03, 80-1007017-01, 49-1000016-04, 49-1000064-02 and 49-1000294-05), 6510 FC Switch (P/Ns 80-1005232-03, 80-1005267-03, 80-1005268-03, 80-1005269-03, 80-1005271-03 and 80-1005272-03), 6520 FC Switch (P/Ns 80-1007245-03, 80-1007246-03, 80-1007242-03, 80-1007244-03, 80-1007257-03), 7800 Extension Switch (P/Ns 80-1002607-07, 80-1006977-02, 80-1002608-07, 80-1006980-02, 80-1002609-07 and 80-1006979-02)} with FIPS Kit P/N Brocade XBR-000195; Firmware Version: Fabric OS v7.2.1 (P/N 63-1001421-01)
2385	05/22/2015	µMACE	Motorola Solutions, Inc.	Hardware Version: P/N AT58Z04; Firmware Version: R01.07.01

Certificate Number	Validation / Posting Date	Module Name(s)	Vendor Name	Version Information
2386	05/22/2015	Hitachi Virtual Storage Platform (VSP) Encryption Engine	Hitachi, Ltd.	Hardware Version: R800L1; Firmware Version: 02.09.28.00 and 02.09.32.00
2387	05/22/2015	HP XP7 Encryption Ready Disk Adapter (eDKA) Level1	Hewlett-Packard Company	Hardware Version: R800L1; Firmware Version: 02.09.28.00 and 02.09.32.00
2388	05/28/2015	IOS Common Cryptographic Module (IC2M) Rel5	Cisco System, Inc.	Firmware Version: Rel 5