Exelon Generation®

James A. FitzPatrick NPP
P.O. Box 110
Lycoming, NY 13093

William C. Drews
Regulatory Assurance Manager

JAFP-18-0082
September 7, 2018

U.S. Nuclear Regulatory Commission
ATTN: Document Control Desk
Washington, DC 20555

James A. FitzPatrick Nuclear Power Plant
Renewed Facility Operating License No. DPR-59
NRC Docket No. 50-333

Subject: Update to Electronic Transmission of Safeguards Information

References: NRC Regulatory Issue Summary, NRC Approval of Commercial Data Encryption Systems for the Electronic Transmission of Safeguards Information, RIS 2002-15 Revision 1, dated January 26, 2006 (ML050460031)

Dear Sir or Madam:

Pursuant to the requirements of 10 CFR 73.22(f)(3) and the guidance provided in NRC Regulatory Issue Summary 2002-15 [Reference], James A. FitzPatrick Nuclear Power Plant (JAF) requests NRC approval to use Symantec Desktop Email Version 10.3.2. This version of encryption product was developed with PGP Software Developer's Kit (SDK) Cryptographic Module Software Version 4.2.1 and complies with Federal Information Processing Standard (FIPS) 140-2 as validated by the National Institute of Standards and Technology (NIST) Consolidated Certificate Number 0014 (Enclosure).

An information protection system for Safeguards Information (SGI) that meets the requirements of 10 CFR 73.21 has been established and is being maintained. Written procedures are in place which describe: 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; and how the identity and, access authorization of the recipient will be verified.

Processing Safeguards Information on electronic systems is performed in accordance with the provisions of 10 CFR 73.22(g). JAF and the Exelon Generation Company, LLC (EGC) Corporate Offices maintain a single (one) public key named with the following syntax:

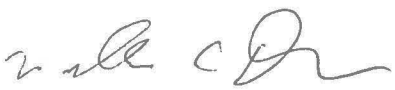
Sullivan_Gregory_Fitzpatrick.asc

This represents the organizational point of contact indicated as owning the key-pair. JAF controls each private key as Safeguards Information. JAF exchanges encrypted Safeguards Information only with the Nuclear Regulatory Commission (NRC), Nuclear Energy Institute (NEI), and other Safeguards Information holders that have received NRC approval to use PGP software.

Wayne Laudenbach, Manager, Security Engineering, is responsible for the overall implementation of the Safeguards Information encryption program for EGC and is also responsible for collecting, safeguarding, and disseminating the software tools needed for encryption and decryption of Safeguards Information.

There are no new regulatory commitments contained in this letter. If you have any questions concerning, please contact William Drews, Regulatory Assurance Manager, at (315) 349-6562.

Sincerely,



William C. Drews
Regulatory Assurance Manager

WD/mh

Enclosure: FIPS 140-2 Consolidated Certificate No. 0014

cc:
NRC Regional Administrator, Region I
NRC Resident Inspector
NRC Project Manager

JAFP-18-0082
Enclosure

FIPS 140-2 Consolidated Certificate No. 0014

(4 Pages)

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. 0014

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: _____

Dated: 3/7/2012

Chief, Computer Security Division
National Institute of Standards and Technology

Signed on behalf of the Government of Canada

Signature: _____

Dated: 12 march 2012

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
1670	02/02/2012	CAT862 Dolby JPEG 2000/MPEG-2 Media Block IDC	Dolby Laboratories, Inc.	Hardware Versions: P/N CAT862Z, Revisions FIPS_1.0, FIPS_1.1, FIPS_1.2 and FIPS_1.3; Firmware Version: 4.4.0.37
1671	02/06/2012	CryptoCore Module	Sensage, Inc.	Software Version: 1.0
1672	02/06/2012	IBM® z/OS® Version 1 Release 13 ICSF PKCS#11 Cryptographic Module	IBM Corporation	Hardware Version: CPACF (P/N COP) and optional 4765-001 (P/N 45D6048); Software Version: ICSF level HCR7780 w/ APAR OA36882 and RACF level HRF7780; Firmware Version: CPACF (FC3863 w/ System Driver Level 86E) and optional 4765-001 (e1ced7a0)
1673	02/06/2012	Secure Router 2330	Avaya, Inc.	Hardware Version: Chassis: 2330, Interface Cards: 2-port T1/E1 Small Card (Assembly Number: 333-70225-01 Rev 4); 2-port Serial Small Card (Assembly Number: 333-70240-01 Rev 02.0011); 1-port ADSL2+ Annex A Small Card (Assembly Number: 333-70260-01 Rev 01); Firmware Version: 10.3.0.100

Certificate Number	Validation / Posting Date	Module Name(s)	Vendor Name	Version Information
1674	02/06/2012	Secure Router 4134	Avaya, Inc.	Hardware Version: Chassis: 4134, Interface Cards: 2-port T1/E1 Small Card (Assembly Number: 333-70225-01 Rev 4); 2-port Serial Small Card (Assembly Number: 333-70240-01 Rev 02.0011); 1-port ADSL2+ Annex A Small Card (Assembly Number: 333-70260-01 Rev 01); 1-port HSSI Medium Card (Part Number: 333-70290-01 Rev 9); 1-port Channelized / Clear Channel T3 Medium Card (Part Number: 333-70280-01 Rev 8); 8-port T1/E1 Medium Card (Part Number: 333-70275-01 Rev 01.0012); 10-port Gigabit Ethernet (GbE) Medium Card (Part Number: 333-70330-01 Rev 01.0023); 24-port Fast Ethernet (FE) Medium Card (Part Number: 333-70325-01 Rev 15); 24-port Fast Ethernet/Power over Ethernet (FE/PoE) Medium Card (Part Number: 333-70325-02 Rev 01.0017); Firmware Version: 10.3.0.100
1675	02/06/2012	Uplogix 430 [1] and 3200 [2]	Uplogix, Inc.	Hardware Versions: (43-1002-50 and 43-1102-50) [1] and (37-0326-03 and 37-0326-04) [2]; Firmware Version: 4.3.5.19979
1677	02/09/2012	McAfee Endpoint Encryption Disk Driver Cryptographic Module 1.0	McAfee, Inc.	Software Version: 6.1.3
1678	02/09/2012	StarSign Crypto USB Token powered by Sm@rtCafé Expert 6.0	Giesecke & Devrient	Hardware Version: P5CC081; Firmware Version: Sm@rtCafT Expert 6.0
1679	02/14/2012	CN1000 Fibre Channel Encryptor	Senetas Corporation Ltd.	Hardware Version: A5175B; Firmware Version: 1.9.3
1680	02/14/2012	Absolute Encryption Engine	Absolute Software Corporation	Software Version: 1.2.0.46

Certificate Number	Validation / Posting Date	Module Name(s)	Vendor Name	Version Information
1681	02/28/2012	PGP Software Developer's Kit (SDK) Cryptographic Module	Symantec Corporation	Software Version: 4.2.1
1682	02/14/2012	Voltage IBE Cryptographic Module	Voltage Security, Inc.	Software Version: 4.0
1683	02/15/2012	Communication Server	Lenel Systems International, Inc.	Software Versions: 5.12.110, 6.0.148, 6.1.22, 6.3.249 or 6.4.500
1684	02/24/2012	PGP Cryptographic Engine	Symantec Corporation	Software Version: 4.2.1