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

April 16, 2019

MEMORANDUM TO: James G. Danna, Chief
Plant Licensing Branch I
Division of Operating Reactor Licensing
Office of Nuclear Reactor Regulation

FROM: Carleen J. Parker, Project Manager ***/RA/***
Plant Licensing Branch I
Division of Operating Reactor Licensing
Office of Nuclear Reactor Regulation

SUBJECT: JAMES A. FITZPATRICK NUCLEAR POWER PLANT – USE OF ENCRYPTION SOFTWARE FOR ELECTRONIC TRANSMISSION OF SAFEGUARDS INFORMATION (EPID L-2018-LRO-0217)

By letter dated September 7, 2018,[1] Exelon Generation Company, LLC (Exelon or the licensee) submitted a request for an update to the electronic transmission of safeguards information for the James A. FitzPatrick Nuclear Power Plant (FitzPatrick). Specifically, Exelon requested approval to use Symantec Desktop Email Version 10.3.2, which was developed with PGP Software Developer's Kit Cryptographic Module, Software Version 4.2.1, as validated by the National Institute of Standards and Technology Consolidated Certificate Number 0014.

On March 12, 2019,[2] the U.S. Nuclear Regulatory Commission (NRC) staff sent a draft request for additional information by e-mail (copy of draft request for additional information enclosed with this memorandum). The draft request was sent to confirm Exelon's understanding of the information requested.

Subsequently, by letter dated April 8, 2019,[3] Exelon withdrew the request to update the electronic transmission of safeguards information for FitzPatrick. Based on this withdrawal, the NRC staff no longer has a need to issue the draft request for additional information as final.

Based on the above, the NRC staff withdraws its draft request for additional information.

Docket No. 50-333

Enclosure:
Draft Request for Additional Information

[1] Agencywide Documents Access and Management System (ADAMS) Accession No. ML18250A285
[2] ADAMS Accession No. ML19099A285
[3] ADAMS Accession No. ML19098B623

SUBJECT: JAMES A. FITZPATRICK NUCLEAR POWER PLANT – USE OF ENCRYPTION SOFTWARE FOR ELECTRONIC TRANSMISSION OF SAFEGUARDS INFORMATION (EPID L-2018-LRO-0217) DATED APRIL 16, 2019

DISTRIBUTION:
PUBLIC
PM File Copy
RidsNrrLALRonewicz Resource
RidsNrrDorlLpl1 Resource
RidsNrrPMFitzPatrick Resource

ADAMS Accession No.: ML19099A267

OFFICE	NRR/DORL/LPL1/PM	NRR/DORL/LPL1/LA	NRR/DORL/LPL1/BC	NRR/DORL/LPL1/PM
NAME	CParker	LRonewicz	JDanna (JTobin for)	CParker
DATE	04/16/2019	04/10/2019	04/16/2019	04/16/2019

OFFICIAL RECORD COPY

ENCLOSURE

Draft Request for Additional Information Regarding Request to Update Electronic Transmission of Safeguards Information for the James A. FitzPatrick Nuclear Power Plant

DRAFT

REQUEST FOR ADDITIONAL INFORMATION

REGARDING REQUEST TO UPDATE ELECTRONIC TRANSMISSION

OF SAFEGUARDS INFORMATION

EXELON GENERATION COMPANY, LLC

JAMES A. FITZPATRICK NUCLEAR POWER PLANT

DOCKET NO. 50-333

By letter dated September 7, 2017,[1] Exelon Generation Company, LLC (Exelon or the licensee) submitted a request for an update to the electronic transmission of safeguards information (SGI) for the James A. FitzPatrick Nuclear Power Plant (JAF). Specifically, Exelon requests approval to use Symantec Desktop Email Version 10.3.2, which was developed with PGP Software Developer's Kit Cryptographic Module, Software Version 4.2.1, as validated by the National Institute of Standards and Technology (NIST) Consolidated Certificate Number 0014. Consolidated Certificate Number 0014, includes NIST Certificate Number 1681, "PGP Software Developer's Kit Cryptographic Module, Software Version 4.2.1."

As a matter of practice, and for information protection purposes, the NRC has adopted a policy of only approving NIST cryptographic modules that have an "active" status as stated in the NIST Cryptographic Module Validation Program. We encourage NRC licensees, certificate holders and applicants that seek initial NRC approval, as prescribed by Title 10 of *The Code of Federal Regulations* (10 CFR), Section 73.22(f)(3), to rely on cryptographic modules that have an active status in the NIST Cryptographic Module Validation Program.

Certificate Number 1681 has been moved to the 'historical' section of NISTs validated modules. If a validated certificate is marked as historical, it does not mean the overall Federal Information Processing Standards (FIPS) -140 certificate has been revoked. Rather, it indicates that the certificate and the documentation posted with it is more than 5 years old and has not been updated to reflect the latest guidance and/or transitions, and may not accurately reflect how the module can be used in FIPS mode. That limitation hampers the NRC's ability to make an informed decision as to how the software will be used, consistently, to transmit in a FIPS mode that is compliant.

NISTs websites states that Federal Agencies should not include historical certificates when making new procurements. Those Agencies that possess NIST historical module certificates may make a risk determination on whether to continue using a module, which is historical, based on their own assessment of where and how the module is used. While JAF is not a Federal Agency, the spirit and intent of the NIST guidance is carried forward as the NRC makes a concerted effort to ensure that SGI is protected during electronic transmission.

[1] Agencywide Document Access and Management System Accession No. ML18250A285

Licensees, certificate holders and applicants that currently possess historical NIST validated certificates, previously approved by the NRC for the secure transmission of SGI, should make a risk determination, in accordance with NIST's website, on whether to continue using the validated module. That determination should be based on their own assessment of where and how the module is used.

The U.S. Nuclear Regulatory Commission (NRC or the Commission) staff has reviewed the request and, based upon this review, determined that the following additional information is needed to complete our review:

1. Does JAF have a risk assessment process for identifying cyber risk?
    a. Describe the process that is used;

2. Has JAF contacted Symantec to determine if the FIPS mode guidance (i.e. how it can be used) as stated at the time of NIST validation, is the latest guidance?
    a. If JAF did not contact Symantec, explain the rationale for not contacting the software developer.
    b. If JAF did contact Symantec, summarize the guidance that was provided, and explain how JAF intends to implement that guidance.

3. Does JAF have procedures in place that only allow SGI cleared personnel to operate or conduct maintenance on the stand-alone system used to process SGI?

4. Has the stand-alone system, used to process SGI, been a part of an inquiry into a malicious or benign attempt to gain unauthorized access or purposeful attempt to circumvent established system security procedures? If so, describe the mitigation process that took place.

5. Does JAF have policies or procedures in place that identify or control the process for the introduction of software or hardware to the stand-alone system that will operate the Symantec software?