



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

June 12, 2018

Mr. Daniel G. Stoddard
Senior Vice President and Chief Nuclear Officer
Innsbrook Technical Center
5000 Dominion Blvd.
Glen Allen, VA 23060

SUBJECT: DOMINION ENERGY KEWAUNEE, INC.; DOMINION NUCLEAR CONNECTICUT, INC.; VIRGINIA ELECTRIC AND POWER COMPANY; KEWAUNEE POWER STATION; MILLSTONE POWER STATION UNITS 1, 2, AND 3; NORTH ANNA POWER STATION UNITS 1 AND 2; SURRY POWER STATION UNITS 1 AND 2; AND ASSOCIATED INDEPENDENT SPENT FUEL STORAGE INSTALLATIONS - USE OF ENCRYPTION SOFTWARE FOR ELECTRONIC TRANSMISSION OF SAFEGUARDS INFORMATION

Dear Mr. Stoddard:

By letter dated June 16, 2016 (Agencywide Documents Access and Management System (ADAMS) Accession No. ML16175A572), Dominion Energy Kewaunee, Inc. (DEK), Dominion Nuclear Connecticut, Inc. (DNC), and Virginia Electric and Power Company (Dominion) requested U.S. Nuclear Regulatory Commission (NRC) approval to use the Cellcrypt Mobile application, which uses the cryptographic module identified as Cellcrypt Secure Core 3 FIPS 140-2 Module, Version 2.0.10 by Cellcrypt to transmit Safeguards Information (SGI) via mobile telephone devices. Your request for NRC approval was submitted in accordance with 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). Your request was accompanied with an attachment that contained Consolidated Validation Certificate No. 2575.

Paragraph 73.22(f) of Title 10 of the *Code of Federal Regulations* (10 CFR), "External transmission of documents and material," prescribes 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

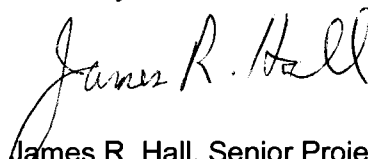
assurance that Safeguards Information is protected before and after transmission.

The NRC staff finds that the use of the Cellcrypt Mobile application is acceptable for processing and transmitting SGI electronically provided that:

1. The Cellcrypt Mobile application has been developed with Cellcrypt Secure Core 3 FIPS 140-2 Module, Version 2.0.10, which has been validated by the National Institute of Technology (NIST) Certificate Number 2575, 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. DEK, DNC, and Dominion facilities licensed by the NRC may replace the current version of encryption product that is 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 uses the same cryptographic module as the current version of encryption product, i.e., document that the FIPS validation certificate of the new version of encryption product, is the same as the current version of encryption product.

The NRC point of contact regarding the use of encryption software for the processing and transmission of SGI is Robert L. Norman, Sr. Program Manager for SGI, Division of Security Operations. Mr. Norman can be reached at (301) 415-2278 or via email at Robert.Norman@nrc.gov.

Sincerely,



James R. Hall, Senior Project Manager
Plant Licensing Branch II-1
Division of Operating Reactor Licensing
Office of Nuclear Reactor Regulation

Docket Nos. 50-305, 50-245, 50-336, 50-423
50-280, 50-281, 50-338, 50-339

cc: Listserv

SUBJECT: DOMINION ENERGY KEWAUNEE, INC.; DOMINION NUCLEAR CONNECTICUT, INC.; VIRGINIA ELECTRIC AND POWER COMPANY; KEWAUNEE POWER STATION; MILLSTONE POWER STATION UNITS 1, 2, AND 3; NORTH ANNA POWER STATION UNITS 1 AND 2; SURRY POWER STATION UNITS 1 AND 2; AND ASSOCIATED INDEPENDENT SPENT FUEL STORAGE INSTALLATIONS - USE OF ENCRYPTION SOFTWARE FOR ELECTRONIC TRANSMISSION OF SAFEGUARDS INFORMATION DATED JUNE 12, 2018

DISTRIBUTION:

PUBLIC
 PM File Copy
 RidsACRS_MailCTR Resource
 RidsNrrDorl Resource
 RidsNrrDorlLpl2-1 Resource
 RidsNrrLAKGoldstein Resource
 RidsNrrPMNorth Anna Resource
 RidsNrrPMSurry Resource
 RidsNrrPMMillstone Resource
 RidsRgnIIMailCenter Resource
 DParsons, NSIR
 RNorman, NSIR

ADAMS Accession No. ML18159A302

***via e-mail**

OFFICE	LPLII-1/PM	LPLII-1/LA	NSIR/DSO/ISB/BC	LPLII-1/BC	LPLII-1/PM
NAME	JRHall	KGoldstein	DParsons*	MOrenak (for MMarkley)	JRHall
DATE	6/12/18	06/11/18	6/8/18	6/12/18	6/12/18

OFFICIAL RECORD COPY