

May 5, 2004

Stephen D. Floyd
Vice President, Regulatory Affairs
Nuclear Generation Division
Nuclear Energy Institute (NEI)
1776 I Street, Suite 400
Washington, DC 20006-3708

SUBJECT: REQUEST FOR USE OF ENCRYPTION SOFTWARE FOR PROCESSING
SAFEGUARDS INFORMATION — NEI PROJECT NUMBER 689

Dear Mr. Floyd:

I am responding to your February 23, 2004, and March 26, 2004, letters in which you requested, on behalf of the industry, U.S. Nuclear Regulatory Commission (NRC) approval to use encryption software for transmission of safeguards information (SGI). You also provided a Nuclear Energy Institute (NEI) developed procedure on the use of encryption software for management and transmission of safeguards information (SGI) (Enclosure 1 — Use of Encryption Software for Management and Transmission of Safeguards Information, dated February 2, 2004) among power reactor licensees, materials licensees with SGI programs, NEI, and the NRC staff.

In Regulatory Issue Summary (RIS) 2002-15, "NRC Approval of Commercial Data Encryption Systems for the Electronic Transmission of Safeguards Information," dated August 28, 2002, the NRC staff provided guidance to all authorized recipients and holders of sensitive unclassified SGI on how to obtain NRC approval of commercial data encryption systems for the electronic transmission of SGI. RIS 2002-15 also outlines the criteria for selecting data encryption software. Specifically, data encryption software should be tested and approved by the National Institute of Standards and Technology (NIST) in accordance with the criteria of Federal Information Processing Standard (FIPS) 140-1 and FIPS 140-2. A list of NIST-approved data encryption software is posted on the NIST website at www.nist.gov.

The guidance in RIS 2002-15 remains relevant today, except that the NRC staff has now concluded that employing electronic data encryption for the transmission of SGI between authorized holders and the NRC is feasible and desirable. Electronic data encryption for the transmission of SGI among authorized SGI holders is consistent with current regulations as summarized in RIS 2002-15.

Authorized SGI holders who wish to employ electronic data encryption for the transmission of SGI should submit a written request for NRC approval consistent with the guidance in RIS 2002-15. This request should also identify the intended recipient(s) of the encrypted SGI data, the individual responsible for collecting, safeguarding, and disseminating (within the authorized SGI holder's organization) the software tools needed for encryption and decryption of SGI, and the means by which the authorized SGI holder intends to confirm that the requirements of 10 CFR Part 73.21(a) and applicable NRC Orders for protection of SGI continue to be satisfied. Enclosure 2 to this letter is provided as a sample request form. Requests should be submitted by individual licensees.

To ensure applicable records management requirements are met, correspondence exchanged via electronic media is subject to the records and distribution requirements normally applied to paper correspondence except as provided under the new NRC rule on electronic submission of information (68 Federal Register 58792, October 10, 2003). As such, electronic submissions of SGI made to the NRC pursuant to the regulations (i.e., submissions made to support licensing actions) may only be submitted on CD-ROM. Please refer to www.nrc.gov/site-help/guid-elec-submission.pdf for additional guidance. The use of data encryption software to transmit SGI using electronic mail is intended only to provide an informal means for timely exchange of information between the NRC and authorized holders of SGI.

NRC approval of requests to use data encryption software to transmit SGI is contingent upon the authorized SGI holder's continued compliance with the provisions of 10 CFR 73.21, "Requirements for the Protection of Safeguards Information" and applicable Order requirements. In accordance with 10 CFR 73.21(a), authorized SGI holders are required to establish and maintain an information protection system that satisfies 10 CFR 73.21(b) through (i). Use of NIST-approved data encryption software in conjunction with an information protection system that satisfies 10 CFR 73.21(b) through (i) constitutes a protected communications circuit pursuant to 10 CFR 73.21(g)(3). Compliance with the provisions of 10 CFR 73.21 is subject to inspection by the NRC staff.

Finally, the staff finds the procedure developed by NEI on the use of encryption software for management and transmission of SGI acceptable with modifications (see Enclosure 2). This modified procedure may be adopted by authorized SGI holders as an acceptable, standardized process for the encryption and exchange of SGI among authorized SGI holders, and between authorized SGI holders and the NRC.

It is our understanding that initially NEI will coordinate and manage the collection and distribution of public encryption keys among interested SGI holders within the nuclear power industry.

The NRC point of contact for all matters pertaining to SGI encryption (including NRC public encryption key coordination) and transmission is Mr. Louis Grosman (NRC/OCIO) who can be reached at (301) 415-5826 or E-mail: lhg@nrc.gov. For matters pertaining to the requirements of 10 CFR Part 73.21 and Orders on SGI protection, the NRC point of contact is Ms. Lynn Silvious (NRC/NSIR) who can be reached at (301) 415-2214 or E-mail: als@nrc.gov.

Sincerely,

/RA/ by Michael F. Weber /f/

Roy P. Zimmerman, Director
Office of Nuclear Security
and Incident Response

Enclosures: As stated

To ensure applicable records management requirements are met, correspondence exchanged via electronic media is subject to the records and distribution requirements normally applied to paper correspondence except as provided under the new NRC rule on electronic submission of information (68 Federal Register 58792, October 10, 2003). As such, electronic submissions of SGI made to the NRC pursuant to the regulations (i.e., submissions made to support licensing actions) may only be submitted on CD-ROM. Please refer to www.nrc.gov/site-help/guid-elec-submission.pdf for additional guidance. The use of data encryption software to transmit SGI using electronic mail is intended only to provide an informal means for timely exchange of information between the NRC and authorized holders of SGI.

NRC approval of requests to use data encryption software to transmit SGI is contingent upon the authorized SGI holder's continued compliance with the provisions of 10 CFR 73.21, "Requirements for the Protection of Safeguards Information" and applicable Order requirements. In accordance with 10 CFR 73.21(a), authorized SGI holders are required to establish and maintain an information protection system that satisfies 10 CFR 73.21(b) through (i). Use of NIST-approved data encryption software in conjunction with an information protection system that satisfies 10 CFR 73.21(b) through (i) constitutes a protected communications circuit pursuant to 10 CFR 73.21(g)(3). Compliance with the provisions of 10 CFR 73.21 is subject to inspection by the NRC staff.

Finally, the staff finds the procedure developed by NEI on the use of encryption software for management and transmission of SGI acceptable with modifications (see Enclosure 2). This modified procedure may be adopted by authorized SGI holders as an acceptable, standardized process for the encryption and exchange of SGI among authorized SGI holders, and between authorized SGI holders and the NRC.

It is our understanding that initially NEI will coordinate and manage the collection and distribution of public encryption keys among interested SGI holders within the nuclear power industry.

The NRC point of contact for all matters pertaining to SGI encryption (including NRC public encryption key coordination) and transmission is Mr. Louis Grosman (NRC/OCIO) who can be reached at (301) 415-5826 or E-mail: lhg@nrc.gov. For matters pertaining to the requirements of 10 CFR Part 73.21 and Orders on SGI protection, the NRC point of contact is Ms. Lynn Silvius (NRC/NSIR) who can be reached at (301) 415-2214 or E-mail: als@nrc.gov.

Sincerely,
/RA/ by Michael F. Weber /f/
 Roy P. Zimmerman, Director
 Office of Nuclear Security
 and Incident Response

Enclosures: As stated

DISTRIBUTION:

WKane	SCollins	C. Pederson	W. Lanning	J. Dyer	C. Casto
H. Miller	L. Reyes	J. Caldwell	B. Mallett	AHowell	T. Marsh
ELeeds	V. Ordaz	M. Layton	G. West	S. Morris	A. Madison
R. Warren	B. Westreich	L. Silvius	DNS r/f	NSIR Mailroom (NSIR-04-0047)	

Package: ML041180611; Response: ML041180613; Encl 1: ML041180614; Encl 2: ML041180622

*See Previous Concurrence

OFC	RSS/DNS*	SC:RSS*	SC:ISS*	OCIO*	OCIO*	OCIO*
NAME	JPeralta:tj	SMorris	LSilvius	LGrosman	KLyons-Burke	ALevin
DATE	4/ 27 /04	4/27/04	04 /29/04	04/29/04	04/29/04	04/29/04
OFC	PD:NSPP*	PD:NSOP*	OGC*	D:DNS/NSIR*	D:NSIR	
NAME	JShea	RWay; for M. Weber	JGoldberg: for J. Heck	GTracy	RPZimmerman	
DATE	4/29/04		5/3/04	5/3/04	5/5 /04	