



Westinghouse Electric Company
Nuclear Power Plants
P.O. Box 355
Pittsburgh, Pennsylvania 15230-0355
USA

U.S. Nuclear Regulatory Commission
ATTENTION: Document Control Desk
Washington, D.C. 20555

Direct tel: 412-374-4663
Direct fax: 412-374-5005
e-mail: PfisteAF@westinghouse.com

Your ref: Project Number 740
Our ref: DCP/NRC1855

March 28, 2007

References: 1. 10 CFR 73.21
2. NRC Regulatory Issue Summary 2002-15

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

Pursuant to the requirements of 10 CFR 73.21(g)(3), Westinghouse Electric Company requests approval to process and transmit Safeguards Information (SGI) using PGP Software (Enterprise, Corporate, or Personal) Desktop Version 8.0 or the latest validated version, developed with PGP SDK 3.0.3. National Institute of Standards and Technology Certificate 394 validates compliance of this SDK with FIPS 140-2 requirements.

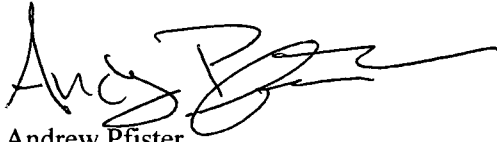
An information protection system for SGI that meets the requirements of 10 CFR 73.21(b) through (i) has been established and is being maintained. Prior to the first use of encryption software for SGI material, written procedures shall be in place to describe, as a minimum: access controls; where and 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 (for example, notification of all authorized users); and how the identity and access authorization of the recipient will be verified.

Westinghouse Electric Company intends to exchange SGI with the NRC, Nuclear Energy Institute (NEI), and other SGI holders who have received NRC approval to use PGP software. Westinghouse Electric Company is responsible for the overall implementation of the SGI encryption program at Westinghouse Electric Company. Westinghouse Electric Company is responsible for collecting, safeguarding, and disseminating the software tools needed for encryption and disseminating the software tools needed for encryption and decryption of SGI.

Pursuant to 10 CFR 73.21(g)(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 73.21(g)(1) and (2).

Should you have any questions or require additional information, please contact Andrew Pfister at (412) 374-4663.

Sincerely,

A handwritten signature in black ink, appearing to read 'Andrew Pfister', with a long horizontal flourish extending to the right.

Andrew Pfister
Passive Plant Engineering & Security

/Attachment

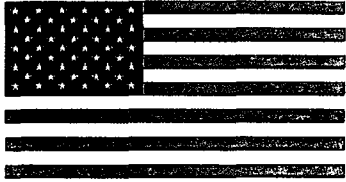
1. "FIPS 140-2 Validation Certificate"

cc:	Juan Peralta	-	NRC/NISR
	Mario Gareri	-	NRC/NSIR
	John Rycyna	-	NEI
	S. Bloom	-	U.S. NRC
	P. Grendys	-	Westinghouse
	D. Lindgren	-	Westinghouse
	E. Schmiech	-	Westinghouse
	R. Bowen	-	Westinghouse

ATTACHMENT 1

“FIPS 140-2 Validation Certificate”

FIPS 140-2 Validation Certificate



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



The Communications Security
Establishment of the Government
of Canada

Certificate No. 494

The National Institute of Standards and Technology, as the United States FIPS 140-2 Cryptographic Module Validation Authority; and the Communications Security Establishment, as the Canadian FIPS 140-2 Cryptographic Module Validation Authority; hereby validate the FIPS 140-2 testing results of the Cryptographic Module identified as:

F-Secure® Cryptographic Library™ by F-Secure Corporation

(When operated in FIPS mode)

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 the above identified cryptographic module 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 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.

This certificate includes details on the scope of conformance and validation authority signatures on the reverse.

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

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 in the product identified as:

F-Secure® Cryptographic Library™ by F-Secure Corporation
(Software Versions: 2.2 (Windows) and 1.1 (Solaris); Software)

Atlan Laboratories, NVLAP Lab Code 200492-0

and tested by the Cryptographic Module Testing accredited laboratory: **CRYPTIK Version 5.8**

is as follows:

Cryptographic Module Specification:	Level 2	Cryptographic Module Ports and Interfaces:	Level 2
Roles, Services, and Authentication:	Level 2	Finite State Model:	Level 2
Physical Security: (Multi-Chip Standalone)	Level N/A	Cryptographic Key Management:	Level 2
EMI/EMC:	Level 2	Self Tests:	Level 2
Design Assurance:	Level 2	Mitigation of Other Attacks:	Level 2
Operational Environment:	Level 2		

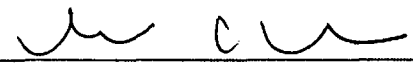
tested in the following configuration(s): Windows 2000 Professional with Service Pack 3 and Q326886 Hotfix EAL 4 on Dell Optiplex GX 400 Personal Computer System, Trusted Solaris 8 7/03 EAL 4 on SunBlade 100

The following FIPS approved Cryptographic Algorithms are used: **DES (Certs. #257 and #259); Triple-DES (Certs. #255 and #257); AES (Certs. #145 and #148); SHS (Certs. #234 and #237); HMAC-SHA-1 and HMAC-SHA-256 (Certs. #234 and #237, vendor affirmed); DSA (Certs. #107 and #109); RSA (Certs. #4 AND #6); RNG (Certs. #2 and #4)**

The Cryptographic module also contains the following non-FIPS approved algorithms: **DES (CTR); Blowfish; CAST-128; MD5; HMAC-MD5; Diffie-Hellman (key agreement); RC2**

Overall Level Achieved: 2

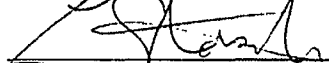
Signed on behalf of the Government of the United States

Signature: 

Dated: 3 July 2005

Chief, Computer Security Division
National Institute of Standards and Technology

Signed on behalf of the Government of Canada

Signature: 

Dated: December 21, 2004

Director, Industry Program Group
Communications Security Establishment