

February 09, 2012

Mr. Eric F. Wilson, CAF Program Manager  
G4S Special Operations  
G4S Secure Solutions USA  
1395 University Blvd  
Jupiter, FL 33458

SUBJECT: USE OF ENCRYPTION SOFTWARE FOR ELECTRONIC TRANSMISSION  
OF SAFEGUARDS INFORMATION

Dear Mr. Wilson:

By letter dated January 5, 2012, G4S Secure Solutions requested approval for the use of Pretty Good Privacy (PGP) Whole Desk Encryption Version 10.1.1, developed with PGP Software Developer's Kit (SDK) 4.0.1 for encryption of Safeguards Information (SGI). National Institute of Standards and Technology (NIST) Certificate (Number 1101) shows that this software development tool complies with Federal Information Processing Standards (FIPS) 140-2, "Security Requirements for Cryptographic Modules."

The U.S. Nuclear Regulatory Commission (NRC) staff finds the use of PGP Whole Desk Encryption Version 10.1.1 is acceptable for processing and transmitting SGI electronically for your site provided that you periodically check the NIST website, <http://csrc.nist.gov/groups/STM/cmvp/documents/140-1/140val-all.htm>, to ensure that the cryptographic algorithm is 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.

Addressees may replace the current version of encryption products that were 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 (i.e., document the FIPS validation certificate of the newer version of encryption product) is the same as the current version of encryption product.

Title 10 of the *Code of Federal Regulations* Paragraph 73.22(f)(3), states in part, ". . . Safeguards Information shall be transmitted outside an authorized place of use or storage only by NRC approved secure electronic devices." The Secretary of Commerce has made use of Cryptographic Module Validation Program products mandatory and binding for Federal agencies when a Federal agency determines that cryptography is necessary for protecting sensitive information.

The public key should be named according to the following syntax: LastName\_FirstName\_Organization.asc. This naming convention represents the organizational point of contact indicated as owning the key. Please provide the public key for transmitting SGI and the point of contact information (name, telephone number and e-mail address) to the NRC point of contact provided below. All SGI holders must employ an appropriate credentialing

E. Wilson

-2-

process to verify that individuals provided with public keys are legitimate users. Private keys must be controlled as SGI.

The NRC technical point of contact regarding the use of mobile telephone devices to transmit SGI is Mrs. Monika Coflin, Cyber Security Specialist, Division of Security Policy, Office of Nuclear Security and Incident Response, and can be reached at (301) 415-6659 or via e-mail at [Monika.Coflin@nrc.gov](mailto:Monika.Coflin@nrc.gov).

If you have any questions, please contact me at (301) 415-5374.

Sincerely,

Craig G. Erlanger, Chief /RA/  
Cyber Security and Integrated Response Branch  
Division of Security Policy  
Office of Nuclear Security and Incident Response

E. Wilson

-2-

process to verify that individuals provided with public keys are legitimate users. Private keys must be controlled as SGI.

The NRC technical point of contact regarding the use of mobile telephone devices to transmit SGI is Mrs. Monika Coflin, Cyber Security Specialist, Division of Security Policy, Office of Nuclear Security and Incident Response, and can be reached at (301) 415-6659 or via e-mail at [Monika.Coflin@nrc.gov](mailto:Monika.Coflin@nrc.gov).

If you have any questions, please contact me at (301) 415-5374.

Sincerely,

Craig G. Erlanger, Chief /RA/  
Cyber Security and Integrated Response Branch  
Division of Security Policy  
Office of Nuclear Security and Incident Response

DISTRIBUTION:

DSP r/f

ADAMS Accession No.: ML120340198, Pkg. ML120340360

OFFICE	NSIR/DSP	NSIR/DSO	NSIR/DSP
NAME	MCoflin	BStapleton	CErlanger
DATE	02/06/11	02/07/2011	02/09/2011

**OFFICIAL RECORD COPY**