NSIR ACTION ITEM COVER SHEET

NSIR ID No. NSIR-12-0021 *EDO Tracking Number (if applicable)*

BACKGROUND INFORMATION

Date Received in NSIR 1/11/2012 *Priority* *Estimated Work Time* *Hrs.*

Document Date 1/5/2012 *Source* Other *Source Author* Eric Wilson, CAF/G

Subject Encryption Software Approval

Action Respond to lettre from G4S regarding validation and approval of encryption software.

Special Instructions:

Due Dates:

EDO *Office* *Division* 2/13/2012

CONTACT AND STATUS

Assigned To: DSO *Contact* Holahan/Stapleton

Please add the RidsNsirMailCenter to distribution (for letter/memoranda responses) or CC (for email responses) in order to track and/or close this ticket.

1/11/2012 *11:00 AM*

G4S Secure Solutions USA
1395 University Blvd
Jupiter, FL 33458
Telephone: 330.801.0510
www.g4s.com/us

SUBJECT: Encryption Software Approval

TO: Mr. James T. Wiggins, Director, Office of Nuclear Security and Incident Response

FROM: Eric Wilson, Program Manager, Composite Adversary Force (CAF)

DATE: 01/05/2012

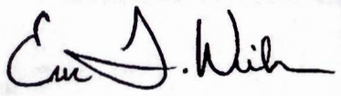
This memorandum is an official inquiry to the NRC requesting validation and approval to use encryption software "Pretty Good Privacy (PGP) Whole Disk Encryption Version 10.1.1". PGP Whole Disk Encryption is a software product that is implemented with the cryptographic functions of the PGP Software Developer's Kit (SDK) Cryptographic Module Version 4.0.1. The PGP SDK Cryptographic Module Version 4.0.1 has been validated and certified to the Federal Information Processing Standards (FIPS) 140-2 current as of 12/29/2011.

PGP Whole Disk Encryption Version 10.1.1 will be installed on standalone laptop computers and the software will operate in FIPS mode. When encrypted safeguards information (SGI) is received, the encrypted information will be removed from the network computer and decrypted on the standalone laptop. Alternately, any SGI sent by G4S will be encrypted on the standalone laptop computer prior to being send via email on any network computer.

Attached are Validated FIPS 140-1 and FIPS 140-2 Cryptographic Modules, the PGP FIPS 140-2 Validation Certification No. 1101, and PGP Whole Disk Encryption Technical Data provided by the PGP Corporation.

POC for this memorandum is the undersigned at 330-801-0510

Eric F. Wilson - CAF Program Manager, G4S Special Operations



Enclosures:

1. Validated FIPS 140-1 and FIPS 140-2 Cryptographic Modules
2. PGP FIPS 140-2 Validation Certification No. 1101
3. PGP Whole Disk Encryption Technical Data provided by the PGP Corporation

Validated FIPS 140-1 and FIPS 140-2 Cryptographic Modules

1995-1997, 1998, 1999, 2000, 2001, 2002, 2003, 2004, 2005, 2006, 2007, 2008, 2009, 2010, 2011,

All

Last Update: 12/29/2011

It is important to note that the items on this list are cryptographic *modules*. A module may either be an embedded component of a product or application, or a complete product in-and-of-itself. If the cryptographic module is a component of a larger product or application, one should contact the product or application vendor in order to determine if their product utilizes an embedded validated cryptographic module. There is inevitably a larger number of security products or applications available which use embedded validated cryptographic modules, than the number of modules which are found in this list. In addition, it is possible that other vendors, who are not found in this list, might incorporate a validated cryptographic module from this list embedded into their own products.

When selecting a module from a vendor, verify that the product or application that is being offered is either a validated cryptographic module itself (e.g. VPN, SmartCard, etc) or the product or application uses an embedded validated cryptographic module (toolkit, etc). Ask the vendor to supply a signed letter stating their application, product or module is a validated module or incorporates a validated module, the module provides all the cryptographic services in the solution, and reference the modules validation certificate number from this listing.

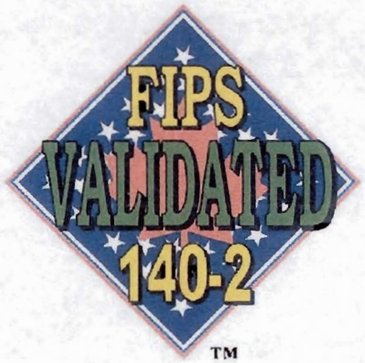
****** NOTE: Module descriptions were provided by the vendors, and their contents have not been verified for accuracy by NIST or CSEC. The descriptions do not imply endorsement by the U.S. or Canadian Governments or NIST. Additionally, the descriptions may not necessarily reflect the capabilities of the modules when operated in the FIPS-Approved mode. The algorithms, protocols, and cryptographic functions listed as "other algorithms" (non-FIPS-Approved algorithms) have not been validated or tested through the CMVP. ******

Questions regarding modules on this list should first be directed to the indicated module vendor.

1101	PGP Corporation, a division of Symantec Corporation 350 Ellis Street Mountain View, CA 94043 USA -Vinnie Moscaritolo TEL: 650-527-8000 FAX: 650-527-1984 **CST Lab:** NVLAP 200802-0	**PGP Software Developer's Kit (SDK) Cryptographic Module** (Software Versions: 4.0.0 and 4.0.1) *(When operated in FIPS mode)* Validated to FIPS 140-2 Security Policy Certificate	Software	03/26/2009; 07/02/2010; 07/30/2010; 01/13/11	***Overall Level:*** 1 -Design Assurance: Level 3 -Operational Environment: Tested as meeting Level 1 with Windows XP Professional SP2; Mac OS X 10.6; Linux, 32-bit: CentOS 5.4 (single-user mode) *-FIPS-approved algorithms:* Triple-DES (Certs. #905, #906 and #907); AES (Certs. #1288, #1289 and #1290); RSA (Certs. #614, #615 and #616); DSA (Certs. #414, #415 and #416); SHS (Certs. #1182, #1183 and #1184); HMAC (Certs. #748, #749 and #750); RNG (Certs. #717, #718 and #719) *-Other algorithms:* AES (EME2 mode; non-compliant); DSA (FIPS 186-3 with SHA-256; non-compliant); CAST-5; IDEA; Two-Fish; Blow-Fish; ARC4-128; MD5; HMAC-MD5; RIPEMD60; ElGamal; RSA (key wrapping; key establishment methodology provides between 112 and 128 bits of encryption strength); Shamir Threshold Secret Sharing Multi-chip standalone "The PGP SDK Cryptographic Module is a FIPS 140-2 validated software only cryptographic module. The module implements the cryptographic functions for PGP products including: PGP Whole Disk Encryption, PGP NetShare, PGP Command Line, PGP Universal, and PGP Desktop. It includes a wide range of field-tested and standards-based encryption, digital signature, and encoding algorithms as well as a variety of secure network protocol implementations. The PGP SDK offers developers this same cryptographic library that is at the heart of PGP products."

FIPS 140-2 Validation Certificate

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



TM

The Communications Security Establishment of the Government of Canada

Certificate No. **1101**

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:

PGP Software Developer's Kit (SDK) Cryptographic Module *by* PGP 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.

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:

PGP Software Developer's Kit (SDK) Cryptographic Module *by* PGP Corporation
(*Software Version: 3.12.0;* Software)

---

and tested by the Cryptographic Module Testing accredited laboratory: ***ÆGISOLVE, INC., NVLAP Lab Code 200802-0***
CRYPTIK Version 7.0
is as follows:

Cryptographic Module Specification:	Level 1	*Cryptographic Module Ports and Interfaces:*	Level 1
Roles, Services, and Authentication:	Level 1	*Finite State Model:*	Level 1
Physical Security: *(Multi-Chip Standalone)*	Level N/A	*Cryptographic Key Management:*	Level 1
EMI/EMC:	Level 1	*Self-Tests:*	Level 1
Design Assurance:	Level 3	*Mitigation of Other Attacks:*	Level N/A
Operational Environment:	Level 1	*tested in the following configuration(s):*	Windows XP Professional SP2; Mac OS X 10.5; Linux, 32-bit: Fedora Core 6 (single-user mode)

The following FIPS approved Cryptographic Algorithms are used: **Triple-DES (Certs. #753, #754 and #755); AES (Certs. #951, #954 and #955); RSA (Certs. #459, #460 and #461); DSA (Certs. #334, #335 and #336); SHS (Certs. #925, #926 and #927); HMAC (Certs. #529, #531 and #532); RNG (Certs. #538, #539 and 540)**

The cryptographic module also contains the following non-FIPS approved algorithms: **AES (EME2 mode; non-compliant); DSA (FIPS 186-3 with SHA-256; non-compliant); CAST-5; IDEA; Two-Fish; Blow-Fish; ARC4-128; MD5; HMAC-MD5; RIPEMD60; ElGamal; RSA (key wrapping; key establishment methodology provides between 112 and 128 bits of encryption strength); Shamir Threshold Secret Sharing**

Overall Level Achieved: 1

Signed on behalf of the Government of the United States

Signature: Dawn F. Dodson for W. Barker

Dated: April 3, 2009

Chief, Computer Security Division
National Institute of Standards and Technology

Signed on behalf of the Government of Canada

Signature:

Dated: March 31, 2009

Director, Industry Program Group
Communications Security Establishment Canada

PGP™ Whole Disk Encryption from Symantec™

High-performance full disk encryption for laptops, desktops, and servers

Data Sheet: Encryption

Benefits

- **Reduces risk of sensitive data exposure from loss or theft** – High-performance full disk encryption for desktops, laptops, and servers.
- **Ensures compliance accountability** – Single, extensible console to define, manage, and automatically enforce encryption security policy with event monitoring and reporting.
- **Simplified day-to-day operations** – Minimizes help desk, administration, and maintenance costs.
- **Easy to use** – Users continue to work as usual. Software automatically encrypts and decrypts data in real-time, without impacting user productivity.

Comprehensive disk encryption

Protecting sensitive data, intellectual property, personal identifiable information (PII) and personal health information (PHI) on laptops, desktops, and removable devices from theft or loss is critical for enterprises and the public sector. Exposure of sensitive data can result in lost intellectual property, fines, legal penalties, and damage to reputation and brand. PGP™ Whole Disk Encryption from Symantec™ provides organizations with comprehensive, multi-platform, and high-performance full disk encryption for all data (user files, swap files, system files, hidden files, and more) on desktops, laptops, and servers. The encrypted data is protected from unauthorized access, providing strong security for intellectual property, customer data, partner data, and brand.

Simple. Fast. Secure. Extensible.

- **Rapid and simple deployment** – From zero to thousands of protected laptops within a matter of weeks.[1] Encrypts hard drives, USB storage devices, and files. Support for Windows®, Mac OS® X, Red Hat®, and Ubuntu®.
- **Simple recovery** – Flexible and easy recovery, including forgotten passphrase options. Supports disaster recovery and planning initiatives, and third-party recovery software.
- **User-friendly** – Background encryption with throttle capabilities. Fewer passwords to remember with support for Windows single sign-on (SSO).
- **Simple and secure day-to-day operations** – Single, centralized policy, key management, and reporting console with web interface manages all clients. Leverages existing infrastructure with Lightweight Directory Access Protocol (LDAP) integration.
- **Strong encryption** – Designed for security and speed, and validated against a number of cryptographic standards.
- **Extensible** – Easily add portable encryption, email encryption, file server, and other encryption applications.

1. Based on typical deployments. Actual organization deployment times may vary.

Rapid deployment

- Flexible .MSI and .PKG formats support most rapid deployment tools such as Systems Management Server®, ZENworks®, and Altiris®.
- Multi-platform: Protects Windows (including Windows Server®), Mac OS X (including Boot Camp®), and Linux® (Ubuntu, Red Hat).
- Silent and invisible enrollment.
- Support for Casper® and other backup software.

Centralized management

- Web-based administration console.
- Enforced user, password, and machine policies.
- Stay-compliant reporting includes machine encryption status, logon failure alerts, and device management.
- Log integration.
- Directory integration through LDAP.
- Strong user key management.

Security and cryptography

- Hardware-based cryptographic acceleration via Intel® Advanced Encryption Standard Instructions (AES-NI) supporting Windows, Mac OS X, and Linux operating systems.
- High-performance, validated, optimized, and strong encryption.
- Built with high-performance Hybrid Cryptographic Optimizer (HCO) technology with Advanced Encryption Standard (AES) 128-bit and 256-bit encryption.
- Smart card (including Personal Identity Verification (PIV) cards), Trusted Platform Module (TPM), and passphrase authentication options.[2]
- Federal Information Processing Standards (FIPS) 140-2 validated, CESG Assisted Products Scheme (CAPS) approved, Defence Infosec Product Co-Operation Group (DIPCOG) approved, Common Criteria Evaluation Assurance Level (CC EAL) 4+ certification.
- Intel® Anti-Theft support available (optional).

Reset passphrase and machine recovery

- Local self-recovery with question-answer authentication avoids help desk calls and does not require network connectivity.
- Secure, one-time use Whole Disk Recovery Token (WDRT).
- Patented, split Additional Decryption Key (ADK) supports corporate access to data and Disaster Recovery and Planning (DRP).
- Machine recovery including support for Windows® Preinstallation Environment (PE) and Bart's Preinstallation Environment (BartPE).
- Support for Guidance® Software EnCase® and AccessData® Forensic Toolkit forensic software.

User-friendly

- Background initial encryption allows users to work as usual without interruption.
- Throttle capability with pause, CPU usage, and power failure safety options.
- Hibernation support on Windows.
- Protects shared systems with multiple users.
- Customizable pre-boot screen.
- Over 50 languages and keyboards supported.
- Windows SSO support.

Technical specification

For complete technical specifications, please visit

http://go.symantec.com/encryption

2. Pre-boot smart card and Trusted Platform Module (TPM) support only on Windows.

Visit our website

http://enterprise.symantec.com

To speak with a Product Specialist in the U.S.

Call toll-free 1 (800) 745 6054

To speak with a Product Specialist outside the U.S.

For specific country offices and contact numbers, please visit our website.

About Symantec

Symantec is a global leader in providing security, storage and systems management solutions to help consumers and organizations secure and manage their information-driven world. Our software and services protect against more risks at more points, more completely and efficiently, enabling confidence wherever information is used or stored.

Symantec World Headquarters

350 Ellis St.
Mountain View, CA 94043 USA
+1 (650) 527 8000
1 (800) 721 3934
www.symantec.com

Symantec helps organizations secure and manage their information-driven world with security management, endpoint security, messaging security, and application security solutions. 21306[illegible] 07/11

Confidence in a connected world. Symantec.