Hughes Network Systems, LLC

Hughes Crypto Kernel

Software Version: 3.1.0.4

FIPS 140-2 Non-Proprietary Security Policy

FIPS Security Level: 1
Document Version: 0.4

Prepared for:

Hughes Network Systems, LLC
11717 Exploration Lane,
Germantown, MD 20876
United States of America

Phone: +1 (301) 428-5500
http://www.hughesnet.com

Prepared by:

Corsec Security, Inc.
10340 Democracy Lane, Suite 201
Fairfax, VA 22030
United States of America

Phone: +1 (703) 267-6050
http://www.corsec.com

Table of Contents

Table of Figures

List of Tables

1 Introduction

1.1 Purpose

This is a non-proprietary Cryptographic Module Security Policy for the Hughes Crypto Kernel (Software version: 3.1.0.4) from Hughes Network Systems, LLC. This Security Policy describes how the Hughes Crypto Kernel meets the security requirements of Federal Information Processing Standards (FIPS) Publication 140-2, which details the U.S. and Canadian Government requirements for cryptographic modules. More information about the FIPS 140-2 standard and validation program is available on the National Institute of Standards and Technology (NIST) and the Communications Security Establishment Canada (CSEC) Cryptographic Module Validation Program (CMVP) website at http://csrc.nist.gov/groups/STM/cmvp.

This document also describes how to run the module in a secure FIPS-Approved mode of operation. This policy was prepared as part of the Level 1 FIPS 140-2 validation of the module. The Hughes Crypto Kernel is referred to in this document as the HCK, the cryptographic module, or the module.

1.2 References

This document deals only with operations and capabilities of the module in the technical terms of a FIPS 140-2 cryptographic module security policy. More information is available on the module from the following sources:

- Hughes corporate website (http://www.hughesnet.com) contains information on the full line of products from Hughes.
- The CMVP website (http://csrc.nist.gov/groups/STM/cmvp/documents/140-1/140val-all.htm) contains contact information for individuals to answer technical or sales-related questions for the module.

1.3 Document Organization

The Security Policy document is one document in a FIPS 140-2 Submission Package. In addition to this document, the Submission Package contains:

- Vendor Evidence document
- Finite State Model document
- Other supporting documentation as additional references

This Security Policy and the other validation submission documentation were produced by Corsec Security, Inc. under contract to Hughes. With the exception of this Non-Proprietary Security Policy, the FIPS 140-2 Submission Package is proprietary to Hughes and is releasable only under appropriate non-disclosure agreements. For access to these documents, please contact Hughes.

2 Hughes Crypto Kernel

2.1 Overview

Geostationary satellite coverage available from Hughes Network Systems, LLC provides the capability to deliver broadband internet service to anywhere around the world. Optimized for broadband IP[1] services, Hughes systems support a wide variety of applications, from high-speed Internet/intranet access, to video conferencing, to voice over IP (VoIP), and adhere to industry standards for voice, video, and serial data protocols. The Hughes HX system is a broadband satellite system, designed and optimized for carrier-grade IP broadband networking and specialized for applications such as mobility and mesh networking. The system includes an economical gateway earth station and high performance remote terminals.

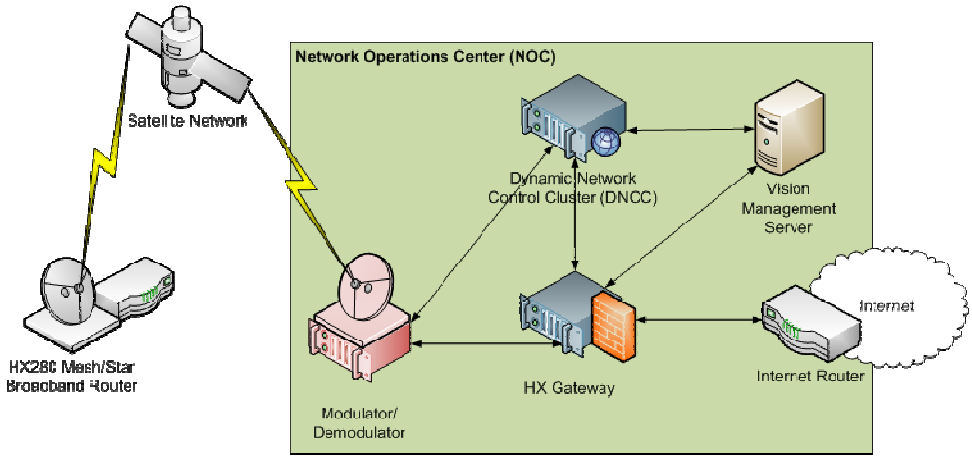

Figure 1 – Hughes HX System Typical Deployment

The HX system provides secure communication with the global IPoS[2] standard over an IPSec[3] protocol, using an array including several specialized HX components. The design of the HX system includes the centralization of cryptographic functionality into a common cryptographic engine called the Hughes Crypto Kernel (HCK). The HCK is used by the following components of the HX systems for internal secure communications:

- HX Gateway: The core component of an HX System deployment is the HX Gateway which acts as the system master and includes the network management and dynamic bandwidth assignment manager. HX Gateways, also called the IP Gateways (IPGWs), are intended to be deployed in a Network Operations Center (NOC) where uplinks to the satellite and Internet infrastructure are available.
- HX280: The HX280 is a high-performance satellite router that enables carrier-grade broadband IP services with enhanced security and on-the-move (OTM) capabilities. The HX280 (Figure 2) is one of several models of broadband satellite routers within the HX System family.

[1] IP – Internet Protocol
[2] IPoS – IP over Satellite
[3] IPSec – IP Security

Figure 2 – HX280 Mesh/Star Broadband Router

HX280 routers are intended to be deployed in the field, acting as the local access points to the satellite communication system and, ultimately, the network infrastructure in a NOC.

- Dynamic Network Control Cluster (DNCC): The DNCC is a high-performance appliance that performs dynamic bandwidth allocation for communications between the HX280s and other HX System appliances. DNCCs are intended to be deployed in the NOC, providing signaling data to the deployed HX280s and the HX Gateway.

The HCK provides the following basic functionalities:

- Creation of dynamically-generated shared session keys using Internet Key Exchange (IKE)
- Establishment and teardown of IPSec tunnels between two or more hosts
- Advanced Encryption Standard (AES) 128- or 256-bit encryption on all data transfer within an IPsec tunnel
- Message authentication and integrity using Keyed-Hash Message Authentication Code (HMAC) with SHA[4]-256

The module provides cryptographic and secure communication services for other applications developed by Hughes as described above. In this document, those applications will be collectively referred as a host application. The Hughes Crypto Kernel is validated at the following FIPS 140-2 Section levels:

Table 1 – Security Level Per FIPS 140-2 Section

Section	Section Title	Level
1	Cryptographic Module Specification	1
2	Cryptographic Module Ports and Interfaces	1
3	Roles, Services, and Authentication	1
4	Finite State Model	1
5	Physical Security	N/A
6	Operational Environment	1
7	Cryptographic Key Management	1
8	EMI/EMC[5]	1
9	Self-tests	1
10	Design Assurance	1

[4] SHA – Secure Hashing Algorithm
[5] EMI/EMC – Electromagnetic Interference / Electromagnetic Compatibility

Section	Section Title	Level
11	Mitigation of Other Attacks	N/A
14	Cryptographic Module Security Policy	1

2.2 Module Specification

The Hughes Crypto Kernel is a software module with a multi-chip standalone embodiment. The overall security level of the module is 1. The physical cryptographic boundary of the Hughes Crypto Kernel is the host platform upon which it runs; however, the module is in the form of a shared library. The HCK has been evaluated and tested for use on a General Purpose Computer (GPC) running the Windows Server 2008 Operating System (OS) in single-user mode

The HCK comprises a single shared library file named "hck.dll". The shared library has separate constituent parts that include: IKE, IPSec, and Common Crypto Interface (CCI) components. The IKE and IPSec components implement a set of protocols developed by the IETF[6] to support secure exchange of packets at the IP layer. The CCI component provides cryptographic functionalities, such as encryption and decryption, random number generation, hashing, and MAC[7]s. The logical cryptographic boundary of the module is shown in Figure 3 and indicated with a teal-colored dotted line.

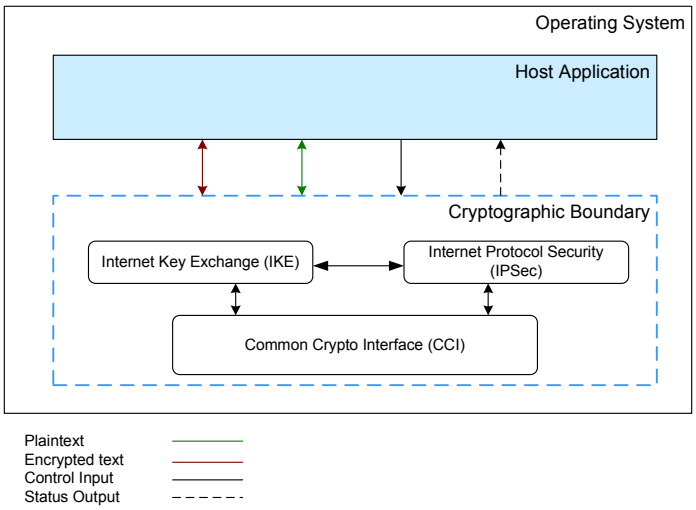

Figure 3 – Hughes Crypto Kernel Cryptographic Boundary

Hck.dll runs on a Windows Server 2008 operating system on a standard server machine which contains integrated circuits on a motherboard, including a Central Processing Unit (CPU), Random Access Memory (RAM), Read Only Memory (ROM), Hard Drive (HD), Local Area Network (LAN) interface, chassis case, power supply, and fans. Figure 4 below is a block diagram of a standard server architecture.

[6] IETF – Internet Engineering Task Force
[7] MAC – Message Authentication Code

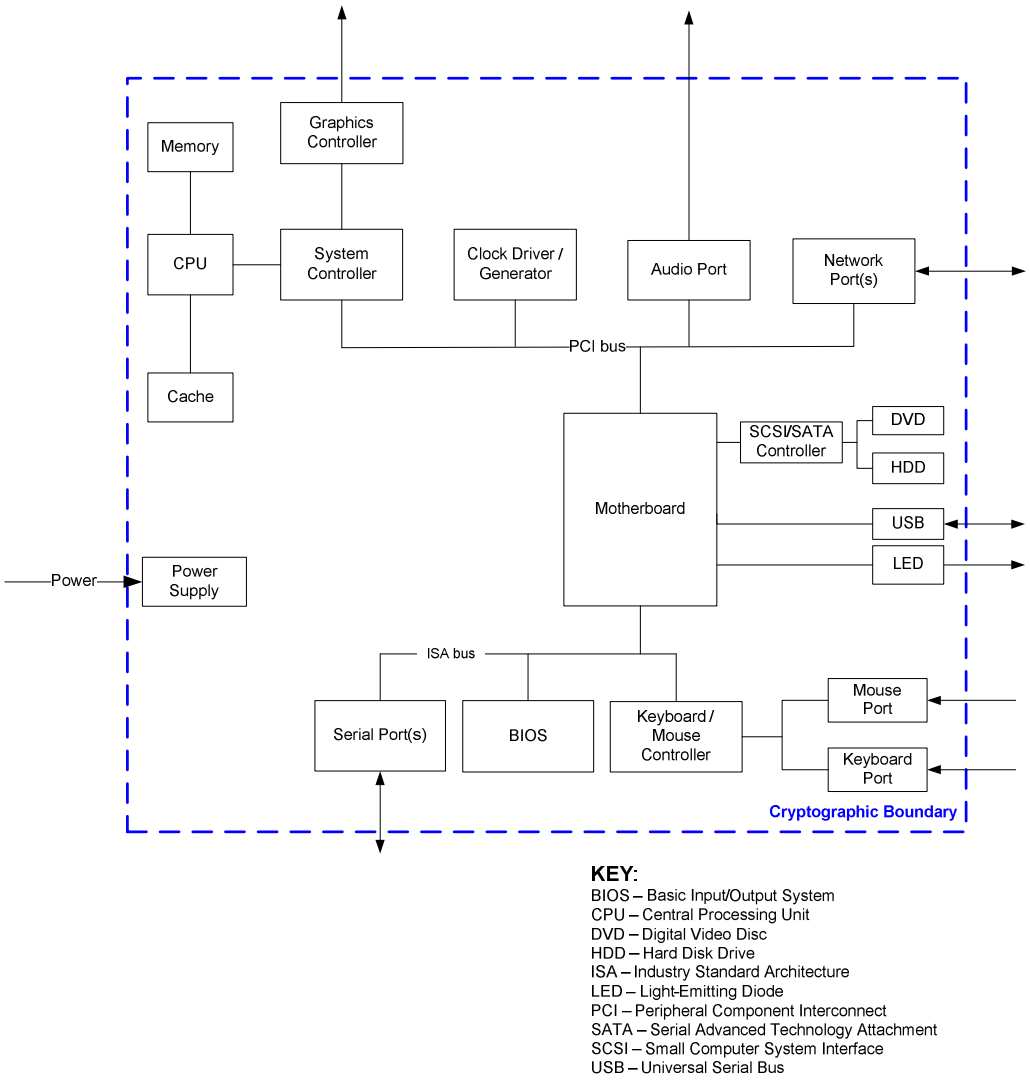

Figure 4 – Standard Server Block Diagram

2.3 Module Interfaces

The HCK implements distinct module interfaces in its software design. Physically, the module ports and interfaces considered to be those of the computer platform that the software runs upon. However, the software/firmware communicates through an Application Programming Interface (API), which allows a host application to access the shared library. Both the APIs and the physical ports in interfaces can be categorized into following logical interfaces defined by FIPS 140-2:

- Data Input Interface
- Data Output Interface
- Control Input Interface
- Status Output Interface

These logical interfaces (as defined by FIPS 140-2) map to the platform's physical interfaces, as described in Table 2. All of these physical interfaces are separated into the logical interfaces required by FIPS 140-2 as described in the following table:

Table 2 – FIPS 140-2 Logical Interface Mappings

FIPS 140-2 Logical Interface	Physical Port/Interface	Hughes Crypto Kernel Port/Interface
Data Input Interface	Keyboard, mouse, DVD drive, and serial/USB/network ports	Arguments for a function that takes the data to be used or processed by the module
Data Output Interface	Monitor and serial/USB/network ports	Arguments for a function that specify where the result of the function is stored
Control Input Interface	Keyboard, DVD drive, mouse, and serial/USB/network port	Function arguments used to control the operation of the module
Status Output Interface	Monitor, LED[8] indicators, and serial/USB/network ports	Return values for function calls or function argument in 'hck_module_status_t' data structure
Power Interface	Power Interface	Not Applicable

2.4 Roles and Services

There are two roles in the module (as required by FIPS 140-2) that operators may assume: a Crypto-Officer role and a User role.

2.4.1 Crypto-Officer Role

The Crypto-Officer (CO) role is responsible for initializing the module, zeroizing keys and CSPs[9], perform self-tests, and monitoring status. Descriptions of the services available to the Crypto-Officer role are provided in the table below. Please note that the keys and CSPs listed in the table indicate the type of access required using the following notation:

- R – Read access: The CSP may be read.
- W – Write access: The CSP may be established, generated, modified, or zeroized.
- X – Execute access: The CSP may be used within an Approved or Allowed security function or authentication mechanism.

[8] LED – Light Emitting Diode
[9] CSP – Critical Security Parameter

Table 3 – Crypto-Officer Services

Service	Description	CSP and Type of Access
hck_init	Validates input parameters before performing power-on self-tests; Initializes configuration	Integrity Test Key – X PRNG seed key – W PRNG seed – W
hck_zeroize_csp	Zeroizes IKE/IPSec ephemeral CSPs	IKE Key Agreement key – W IPSec Traffic key – W IPSec MAC key – W
hck_shutdown	Shuts down all crypto functionality	None
hck_do_self_tests	Performs power-on self-tests	Integrity Test Key – X
hck_get_status	Retrieves the crypto-module status	None
hck_get_name_ver	Retrieves the module name and version number	None
hck_get_version	Retrieves the module's major and minor version numbers	None
hck_get_fips_mode	Determines whether or not FIPS mode has been enabled	None
hck_print_status	Prints module status variables and statistics to a display or log file	None
hck_update_parms	Sets configuration parameters based on module's current mode of operation	PRNG seed key – W PRNG seed – W

2.4.2 User Role

The User role establishes IKE/IPSec sessions and utilizes secure communication functionality provided by the module. Descriptions of the services available to the User role are provided in the table below. Type of access (R, W, or X) is defined in section 2.4.1 of this document.

Table 4 – User Services

Service	Description	CSP and Type of Access
hck_process_ike_event	Ensures that the crypto-module is active and validates input parameters before processing a received IKE packet or provides a timer event to the IKE state machine	Preshared key – R, W, X IPSec Traffic key – W IPSec MAC key – W IKE Key Agreement key – W PRNG seed key – W, X PRNG seed – W, X
hck_process_tx_pkt	Ensures that the crypto-module is active and validates input parameters before processing IPSec transmission packet	IPSec Traffic key – X IPSec MAC key – X PRNG seed key – W, X PRNG seed – W, X

Service	Description	CSP and Type of Access
hck_process_rx_pkt	Ensures that the crypto-module is active and validates input parameters before processing IPSec received packet	IPSec Traffic key – X IPSec MAC key – X PRNG seed key – W, X PRNG seed – W, X
hck_send_ike_msg	Ensures that the crypto-module is active and validates input parameters before invoking IKE transmit function	IKE Key Agreement key – R

2.5 Physical Security

The physical security requirements do not apply since this is a software-only module and does not implement any physical security mechanisms.

The FIPS 140-2 test platform were GPCs running Windows Server 2008 that have been tested for and meet applicable Federal Communications Commission (FCC) Electromagnetic Interference and Electromagnetic Compatibility requirements for business use as defined in Subpart B of FCC Part 15.

2.6 Operational Environment

The software module was tested and found to be compliant with FIPS 140-2 requirements on 32-bit Windows Server 2008. The operating system must be configured for single user mode for FIPS 140-2 compliance (see section 3.1.1 for guidance).

All cryptographic keys and CSPs are under the control of OS, which protects the CSPs against unauthorized disclosure, modification, and substitution. The module only allows access to CSPs through its well-defined APIs. The module performs a Software Integrity Test using the DSA[10] algorithm.

2.7 Cryptographic Key Management

The module implements the FIPS-Approved algorithms listed in Table 5 below.

Table 5 – FIPS-Approved Algorithm Implementations

Algorithm	Certificate Number
AES CBC[11] 128-, 256-bit key	1450
SHA-1, SHA-256	1314
HMAC SHA-1, HMAC-SHA-256	851
DSA (Signature Verification, 1024-bit)	461
ANSI[12] X9.31 PRNG[13] (AES-128)	794

[10] DSA – Digital Signature Algorithm
[11] CBC- Cipher Block Chaining

Additionally, the module utilizes the following non-FIPS-Approved algorithm implementations:

- MD5[14] used in the IKE/IPSec protocol
- Diffie-Hellman key agreement (caveat: 1024-bit Diffie-Hellman key agreement protocol provides 80 bits of encryption strength)

[12] ANSI – American National Standard Institute
[13] PRNG – Pseudo Random Number Generator
[14] MD5 – Message Digest 5

The module supports the critical security parameters (CSPs) listed below in Table 6.

Table 6 – List of Cryptographic Keys, Cryptographic Key Components, and CSPs

Key Type	Generation / Input	Output	Storage	Zeroization	Use
Preshared key	Generated externally, enters the module in plaintext	Never exits the module	Resides in plaintext on volatile memory	Reboot or session termination	Generation of the IPSec Traffic key and Internal IKE authentication
Diffie-Hellman public key	Generated internally	Exits the module in plaintext	Plaintext in volatile memory	Reboot or session termination	Generation of IKE Key Agreement key
Diffie-Hellman private key	Generated internally	Never exits the module	Plaintext in volatile memory	Reboot or session termination	Generation of IKE Key Agreement key
IKE Key Agreement key	Generated during IKE negotiation	Never exits the module	Plaintext in volatile memory	Reboot, session termination, or by calling to 'hck_zeroize_csp' function	Exchanging shared secret during IKE
IPSec Traffic key	Generated during IKE negotiation	Never exits the module	Plaintext in volatile memory	Reboot, session termination, or by calling to 'hck_zeroize_csp' function	Encryption or decryption of IPSec ESP packets
IPSec MAC key	Generated during IKE negotiation	Never exits the module	Plaintext in volatile memory	Reboot, session termination, or by calling to 'hck_zeroize_csp' function	Authentication of IPSec ESP packets
PRNG seed	Generated externally, enters the module via application software	Never exits the module	Plaintext in volatile memory	Reboot, session termination	Random number generation

Key Type	Generation / Input	Output	Storage	Zeroization	Use
PRNG seed key	Generated externally, enters the module via application software	Never exits the module	Plaintext in volatile memory	Reboot, session termination	Random number generation
Integrity Test Key	Generated externally, hard-coded in module	Never exits the module	Hard-coded	N/A	Verification of module integrity

2.8 Self-Tests

The HCK performs a set of self-tests upon power-up and conditionally as required in FIPS 140-2.

2.8.1 Power-Up Self-Tests

Power-up self tests are executed automatically when the module is loaded into memory space. If any of the Self-Tests fail, the module enters an error state and prevents all cryptographic data processing and functionality. The Hughes Crypto Kernel performs the following power-up self-tests:

- Software integrity test using a DSA public key
- Known Answer Tests (KATs)
    - AES 128-, 256-bit key CBC mode KAT (encryption and decryption)
    - SHA-1 and SHA-256 KATs
    - HMAC-SHA-1 and HMAC SHA-256 KATs
    - ANSI X9.31 PRNG KAT

2.8.2 Conditional Self-Tests

The module performs a Continuous RNG Test (CRNGT) for the Approved PRNG to ensure that the 128-bit random result is not equivalent to the previous result.

2.8.3 Critical Functions Self-Tests

At the power-up, the module also tests for the following:

- Minimum available memory on the host device

2.9 Mitigation of Other Attacks

This section is not applicable. The module does not claim to mitigate any additional attacks in its FIPS-Approved mode of operation.

3 Secure Operation

The Hughes Crypto Kernel meets Level 1 requirements for FIPS 140-2. The sections below describe how to place and keep the module in FIPS-Approved mode of operation. Section 3.1 below provides guidance to the Crypto-Officer for managing the module.

3.1 Secure Management

The Hughes Crypto Kernel is distributed by Hughes via secure download or on a CD. The module is a provided to the Crypto-Officer only as part of Hughes' HX system applications and is not distributed as a separate binary. Thus, module operators are not required to perform any steps to ensure that the module is running in its FIPS-Approved mode of operation.

The Crypto-Officer role is responsible for installing the host application (and thus, the module). The host application must first call the function hck_init() to load and initialize the module. This function call is the entry point to the module, and ensures that all necessary power-up self-tests are called. When properly initialized, the HCK will only operate in its defined FIPS-Approved mode of operation. Any use of the module without proper initialization will result in the module operating in a non-Approved manner.

The module implements a software integrity test that consists of a DSA signature computed over the image that comprises the module. During the power-up self-tests phase, the signature is verified over the stored HCK instance. If the stored signature is verified, then the test is passed. Otherwise, the test is failed and the module enters an error state where no cryptographic functionality is allowed.

3.1.1 Initialization

FIPS 140-2 mandates that a software cryptographic module at Security Level 1 shall be restricted to a single operator mode of operation. Prior to installing the module, the Crypto-Officer must ensure the server running Windows Server 2008 is in single-user mode. To configure the OS for single-user mode, the Crypto-Officer must ensure that all remote guest accounts are disabled in order to ensure that only one operator can log into the Windows OS at a time. The services that need to be turned off for Windows are:

- Fast-user switching (irrelevant if server is a domain member)
- Terminal services
- Remote registry service
- Secondary logon service
- Telnet service
- Remote desktop and remote assistance service

3.1.2 Management

The Crypto-Officer should monitor the module's status regularly and make sure only the services listed in Table 3 and Table 4 are being used. If any irregular activity is noticed or the module is consistently reporting errors, then Hughes Network Systems customer support should be contacted.

3.1.3 Zeroization

The module does not persistently store any key or CSPs. All ephemeral keys used by the module are zeroized upon reboot, session termination, or if the Crypto-Officer calls the hck_zeroize_csp function.

3.2 User Guidance

Only the module's cryptographic functionalities are available to the User. Users are responsible to use only the services that are listed in Table 4. Although the User does not have any ability to modify the configuration of the module, they should report to the Crypto-Officer if any irregular activity is noticed.

4 Acronyms

This section lists acronyms used in the document in the following table.

Table 7 – Acronyms

Acronym	Definition
AES	Advanced Encryption Standard
ANSI	American National Standard Institute
API	Application Programming Interface
CBC	Cipher Block Chaining
CCI	Common Cryptographic Interface
CMVP	Cryptographic Module Validation Program
CO	Crypto-Officer
CPU	Central Processing Unit
CRNGT	Continuous Random Number Generator Test
CSEC	Communications Security Establishment Canada
CSP	Critical Security Parameter
DC	Direct Current
DNCC	Dynamic Network Control Cluster
DSA	Digital Signature Algorithm
DVD	Digital Versatile Disc
ECB	Electronic Book Code
EMC	Electromagnetic Compatibility
EMI	Electromagnetic Interference
FIPS	Federal Information Processing Standard
GPC	General Purpose Computer
HCK	Hughes Crypto Kernel
HD	Hard Disk
HMAC	(Keyed-) Hash Message Authentication Code
IETF	Internet Engineering Task Force
IKE	Internet Key Exchange
IP	Internet Protocol
IPGW	IP Gateway
IPoS	IP over Satellite
IPSec	IP Security
KAT	Known Answer Test

Acronym	Definition
LAN	Local Area Network
MAC	Message Authentication Code
MD	Message Digest
NIST	National Institute of Standards and Technology
NOC	Network Operations Center
OS	Operating System
OTM	On-The-Move
PRNG	Pseudo Random Number Generator
RAM	Random Access Memory
ROM	Read Only Memory
SHA	Secure Hash Algorithm
USB	Universal Serial Bus
VoIP	Voice over IP

Prepared by:
Corsec Security, Inc.

10340 Democracy Lane, Suite 201
Fairfax, VA 22030
United States of America

Phone: (703) 267-6050
Email: info@corsec.com
http://www.corsec.com