CyberGuard Cryptographic Module v5.0P1f

For

CyberGuard VPN Firewall

Level 1 Validation

Security Policy

May 8, 2002

(Revised June 12, 2003)

1. Introduction

1.1. Purpose

This document is the non-proprietary Cryptographic Module Security Policy for the CyberGuard Cryptographic Module v5.0P1f.

This Cryptographic Module Security Policy is part of the FIPS 140-1 documentation prepared for validation of the CyberGuard Cryptographic Module v5.0P1f. The CyberGuard Cryptographic Module v5.0P1f provides robust security in a flexible software module, meeting all FIPS 140-1 Level 1 requirements. This security policy describes how the CyberGuard Cryptographic Module v5.0P1f meets the FIPS 140-1 requirements, and how the CyberGuard Cryptographic Module v5.0P1f is securely used within all CyberGuard products.

1.2. Audience

This document is intended for FIPS 140-1 testers, National Institute of Standards and Technology (NIST) and Communications Security Establishment (CSE) reviewers, and customers interested in the CyberGuard Cryptographic Module v5.0P1f's functionality and compliance with FIPS 140-1. This security policy describes the CyberGuard Cryptographic Module using technical terminology associated with computer security and FIPS 140-1. Readers seeking additional information are referred to the following sources for more detailed information about the CyberGuard Cryptographic Module v5.0P1f and how it works with CyberGuard's entire product line; please visit the CyberGuard Web site at:

http://www.cyberguard.com/

For more information about the FIPS 140-1 standard and validation program please visit the NIST Web site at:

http://csrc.nist.gov/cryptval

For answers to technical or sales related questions please refer to the contacts listed on the CyberGuard Web site at:

http://www.cyberguard.com/

2. CyberGuard Cryptographic Module Version 5.0P1f

2.1. Overview

The CyberGuard Cryptographic Module v5.0P1f is a software cryptographic module (CM) that works with our IPSEC Express and VPN functions to provide user authentication and tunnel encryption.

The CyberGuard VPN firewall is a gateway between trusted and non-trusted networks. It is a security gateway, protecting network access (firewall), network visibility (NAT), and network data (VPN). In the figure below, the gateway-to-gateway tunnel connects networks A and B to form a Virtual Private Network (VPN). The host-to-gateway tunnel allows the remote (known as the "road warrior") to connect to the VPN from anywhere Internet access is available. The gateway-to-gateway connection is how the distant and disparate networks of enterprise branch offices are brought together to form the VPN. The VPN host type connection is very popular for use by enterprise telecommuters, a company's mobile sales force, and extranet partner access to protected business-related services provided by the enterprise.

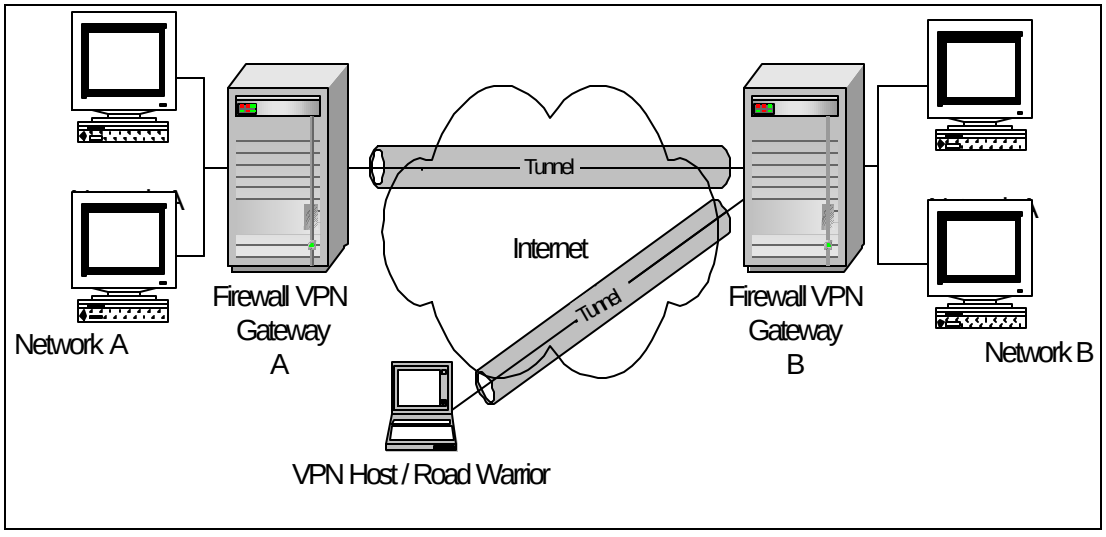


Figure 1 – VPN Connections

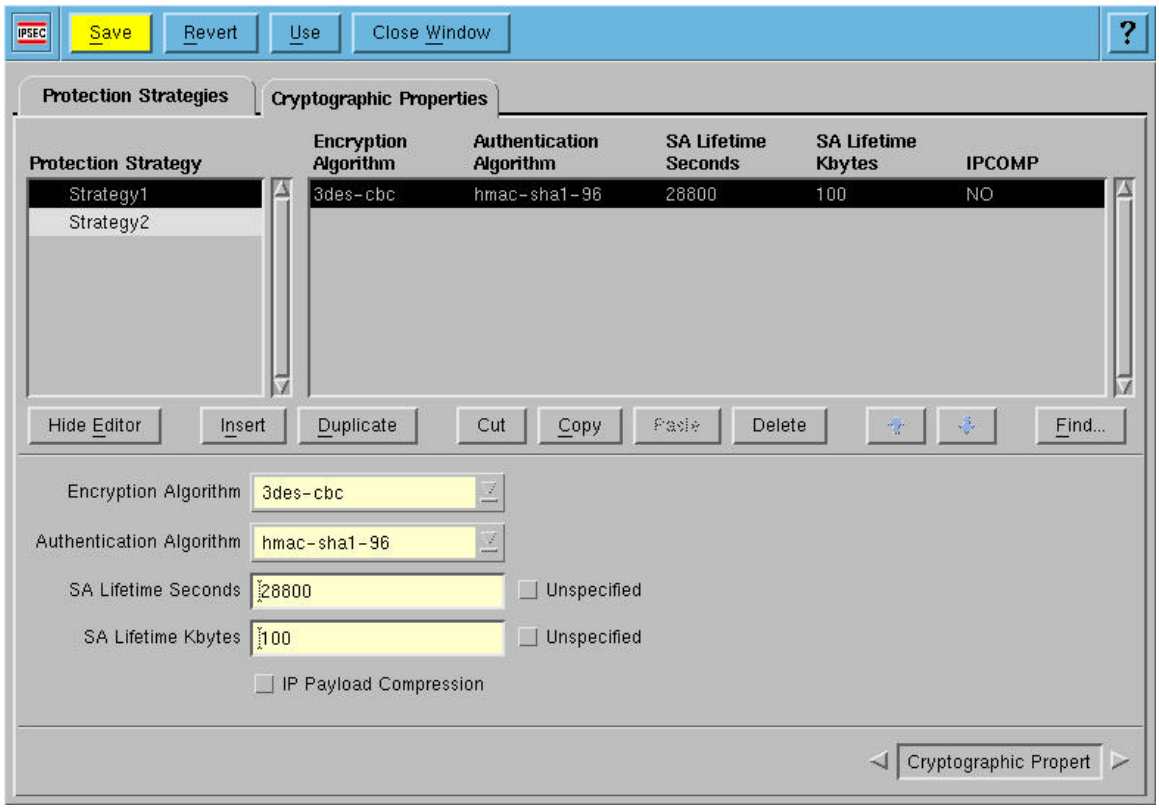
Gateway-to-gateway and VPN host-to-gateway are the two types of connections that are supported by the firewall VPN. It is the purpose of this document to describe the

policy configuration and management required by the firewall VPN to support these connections.

Most VPNs are now based on IP security (IPSec). IPSec secures the data at the network level. It defines a security protocol for both Ipv4 and Ipv6, which automatically protects upper layer protocols (TCP, UPD, etc.) To realize a fast time to market, the SSH IPSec Express™ Toolkit (the toolkit) has been selected.

Note: Throughout this document the endpoints of tunnels may be referred to as the IPSec peers. The security attributes shared between the firewall VPN and the peer is referred to as the VPN secure channel. Typically, it is the remote endpoint relative to the firewall VPN being managed that is referred to as the IPSec peer, or simply the peer. CyberGuard's VPN solution consists of an integrated IPSec packet processing engine with its firewall packet filter (**netguard**) and network address translation (**NAT**) to provide both the secure functionality of a VPN gateway combined with the protection of the firewall.

Window 1 IPSec Protection Strategies window – Cryptographic Properties Tab


IPSEC
Save
Revert
Use
Close Window
?
Protection Strategies
Cryptographic Properties
Protection Strategy
Encryption Algorithm
Authentication Algorithm
SA Lifetime Seconds
SA Lifetime Kbytes
IPCOMP
Strategy1
Strategy2
3des-cbc
hmac-sha1-96
28800
100
NO
Hide Editor
Insert
Duplicate
Cut
Copy
Paste
Delete
Find...
Encryption Algorithm
3des-cbc
Authentication Algorithm
hmac-sha1-96
SA Lifetime Seconds
28800
Unspecified
SA Lifetime Kbytes
100
Unspecified
IP Payload Compression
Cryptographic Propert

This page has the following fields and controls:

Protection Strategy	Displays a list of Protection Strategies defined on the Protection Strategies page. Select a Protection Strategy to configure its cryptographic properties.
Encryption Algorithm	Displays a list of encryption algorithms. The supported algorithms are: **3des-cbc**, **des-cbc**, **aes-cbc**, **twofish-cbc**, **blowfish-cbc**, **cast128-cbc**, and **none**. **none** may be specified only if the **Authentication Algorithm** is not equal to **none**. The default value is **3des-cbc**.
Authentication Algorithm	Displays a list of HMACs. The supported HMACs are: **hmac-sha1-96**, **md5**, **hmac-md5-96**, and **none**. **none** may be specified only if the **Encryption Algorithm** is not equal to **none**. The default value is **hmac-sha1-96**.
SA Lifetime Seconds	Duration of the SA in seconds. The minimum value is **60** (1 minute); the maximum value is **315360000** (10 years); the default value is **28800** (8 hours).
Unspecified	Indicates the Security Association will not be expired based on the **SA Lifetime Seconds** type. Represents a value of **0**. If this box is checked, only **SA Lifetime Kbytes** will be used. **Unspecified** cannot be checked for both **SA Lifetime Seconds** and **SA Lifetime Kbytes**.
SA Lifetime Kbytes	Amount of traffic that can be protected by the SA in Kbytes. The minimum value is **100**; the maximum value is **2147483647**; the default value is **51200** (50 MB).
Unspecified	Indicates the Security Association will not be expired based on the **SA Lifetime Kbytes** type. Represents a value of **0**. If this box is checked, only **SA Lifetime Seconds** will be used. **Unspecified** cannot be checked for both **SA Lifetime Seconds** and **SA Lifetime Kbytes**.
IP Payload Compression	Using the IP Payload Compression algorithm (IPCOMP), compresses IP payload to counteract the overhead introduced by the IPSec protocol.

2.1.1. Configuring the CyberGuard Cryptographic Module v5.0P1f in FIPS mode:

Encryption Algorithm: Select DES (legacy systems only), 3DES (FIPS PUB 46-3: Data Encryption Standard, and Triple DES) or AES (FIPS PUB 197 Advanced Encryption Standard) encryption.

Authentication Algorithm: Select HMAC-SHA-1.

SA Lifetime Seconds: Use default (28800); Unspecified: Unchecked

SA Lifetime Kbytes: Use default (51200); Unspecified: Checked (Forces use of Seconds)

IP Payload Compression: Either checked or unchecked.

The CyberGuard Cryptographic Module v5.0P1f allows users to specify read, write, and update access for each file of the CyberGuard Cryptographic Module v5.0P1f. The CyberGuard Cryptographic Module v5.0P1f will generate DES, 3DES or AES session keys using Diffie-Hellman key agreement. CyberGuard Cryptographic Module v5.0P1f users then execute encrypted sessions using the session key.

2.1.2. Cryptographic Boundary

The CyberGuard Cryptographic Module is a software module. The module was tested on an Intel® SR2100/STL2 server chassis, the physical enclosure of which describes the physical boundary. The logical cryptographic boundary is the *vpnguard* executable.

2.2. Module Interfaces

The CyberGuard Cryptographic Module v5.0P1f is a multi-chip standalone module when in FIPS 140-1 mode. The module is designed for use with one or more Intel Pentium-class CPUs. Physical interfaces are provided by the hardware in the form of Keyboard/console and Ethernet ports. However, once information is processed through these physical interfaces, the CyberGuard Cryptographic Module v5.0P1f provides a logical interface through function calls (API) within the VPN program. Thus, there is a single interface provided by the CyberGuard Cryptographic Module v5.0P1f, which is further logically divided into data input, data output, control input, and status output interfaces. Since it is a software module, the CyberGuard Cryptographic Module v5.0P1f does not provide a separate power or maintenance access interface beyond the power interface provided by the CPU itself.

CyberGuard protects all information in the VPN (**netguard)** portion of the product with the CyberGuard Cryptographic Module, and the CyberGuard VPN firewall uses **Operator Authentication** (prior to initialization) where every operator who is allowed access to the cryptographic module performs an initial authentication sequence using a userID and password to log on to the PC. This authentication is not passed to the cryptographic module.

To perform the services of a cryptographic officer, the operator must perform another log-on to the CyberGuard VPN firewall with a userID and Password unique to that role, which enables the Crypto Officer (CO) to perform any of the CO services.

2.3. Roles and Services

The CyberGuard Cryptographic Module v5.0P1f supports two distinct roles using password authentication for the crypto officer and DSA Signature Authentication for the users.

2.3.1. Authentication Policy

The module uses role based authentication.

The Crypto Officer (CO) authenticates to the CyberGuard Firewall by inserting a password. He must then use a **second password** to gain the privileges to perform CO services on the CyberGuard **Cryptographic Module** v5.0P1f. The user, which is actually another CyberGuard Cryptographic Module v5.0P1f, is authenticated by DSA signature verification.

Role	**Type of Authentication**	**Authentication Data**
User	Role	Digital Signature
Crypto-Officer	Role	UserID/Password

Table 1: Authentication Data

2.3.2. Access Control Policy

The following table defines which user has access to each service.

Role	**Authorized Services**
User	Symmetric Encryption/Decryption -AES -TDES -DES (Legacy systems only) -Twofish (non-FIPS) -Blowfish (non-FIPS) -CAST-128 (non-FIPS) Digital Signature Generation/Verification -DSA Hash Generation -SHA-1 -RipeMD160 (non-FIPS) -Tiger192 (non-FIPS) MAC Generation -HMAC-SHA-1 -HMAC-MD5 (non-FIPS) Key Agreement -Diffie-Hellman (non-FIPS) Random Number Generation -ANSI X9.31-A.2.4
Cryptographic Officer	Initialization of Cryptographic Module FIPS Mode Configuration CSP Input/Output -Module State Zeroization

Table 2: Authorized Services

An operator performing a service for either crypto-officer or user role, accesses the service through the use of the cryptographic API.

Service	Cryptographic Keys/CSPs	Access
Symmetric Encryption/Decryption	Symmetric Key	Read/Write
Digital Signature Generation/Verification	Asymmetric Key Pair	Read/Write
Hash Generation	None	N/A
MAC Generation	Symmetric Key	Read/Write
Key Agreement	Asymmetric Key Pair	Read/Write
Random Number Generation	Seed	N/A
Module Initialization	None	N/A
FIPS Mode Configuration	None	N/A
CSP Input/Output	CSP	Read/Write
Zeroization	Keys/CSP	Read/Write

Table 3: Access Rights (applies to both FIPS and non-FIPS modes)

2.4. Finite State Machine

The CyberGuard Cryptographic Module v5.0P1f is designed around a Finite State Machine Model (FSM) that conforms to all FIPS PUB 140-1 requirements.

2.5. Physical Security

The CyberGuard Cryptographic Module v5.0P1f runs on the CyberGuard Firewall/VPN Revision 5.0P1 for UnixWare version 2.1.3. CyberGuard Firewalls run on any Intel-based PC utilizing a variety of Intel-based processor boards including the Intel STL2 Server board, which is loaded with the Firewall and VPN modules when configured. For FIPS 140-1 purposes, the Cryptographic Module was tested against Level-1 FIPS 140-1 physical security requirements when running on an Intel® SR2100 server with STL2 server board. This board meets all Level-1 requirements, providing a multi-chip standalone module with production grade equipment, standard passivation, and a strong enclosure.

2.6. Software Security

The CyberGuard Cryptographic Module v5.0P1f is a software module within VPN, which follows IPSEC rules.

The CyberGuard Cryptographic Module v5.0P1f is written in C and C++.

The CyberGuard Cryptographic module has the advantage of being integrated within the VPN functionality, which is an extension of the firewall security features. The crypto module is further protected by the functionality of the firewall, which runs on the security-hardened operating system described below.

2.7. Operating System Security

The CyberGuard Cryptographic Module runs on UnixWare version 2.1.3. Access to the operating system is not permitted in FIPS mode.

2.7.1. Configuration in single user mode:

The following OS security hardening measures have been implemented in a package called FIPS1401. This package, when installed, turns the CyberGuard boxes into single user, single processor boxes, removes the shell access so no logins are possible other than the single user login at the firewall, removes the possibility of executing an xterm or invoking a shell in addition to multiple other measures to harden the box to eliminate the possibility of loading/compiling/executing any un-trusted software on the box when in FIPS mode.

In addition, in the FIPS mode, CyberGuard recommends password protecting the BIOS settings of the box so that no changes can occur at the BIOS level and any changes required would be with the knowledge of the operator and require proper password. This will eliminate the possibility of utilizing the floppy or the CD-ROM drives to load unauthorized software. A procedure to this effect is provided. More specific details of the changes are as follows:

2.7.2. General Modifications For OS Lockdown:

A new UW license key will be installed when the fips1401 package is installed (using pkgadd). This license key will license the system for 1 user and 1 processor. This change will turn a multi-user/multi-processor box into a single-user/single-processor box. This action is taken to meet the level 1 requirement of single-processor operating systems.

The real xterm has been removed and instead a fake xterm has been added to the system as part of the FIPS OS lockdown. The fake xterm (invoked when the shell window is accessed) will print a message stating “Unavailable Service in FIPS Mode”. It also has a “Close Window” button. The removal of the xterm behind the shell window is the main point that eliminates the possibility of accessing the OS and performing illegal operations in the FIPS mode.

The operation of the cg_getorders (software update tool through the network) has been modified similarly. When a user presses the “Use” button on the Software Update window, the “Unavailable Service in FIPS Mode” window will pop up and closes within a few seconds. After this window, a dialog pops up that says “Software update finished with errors”. The user will be unable to utilize this window to download software to the firewall.

The ability of console login has been removed from inittab. This eliminates any attempts to login at the console level.

The boot prompt and the boot timeout (during boot up sequence when the box gives you a chance to bypass the automatic boot sequence and go down to maintenance mode) have also been eliminated.

The maintenance kernel (mUNIX) has been removed. This, coupled with disabling the interruption of the boot sequence to go down to the maintenance mode eliminates any possibilities of booting a different kernel.

The firewall alerts allow the configuration of running a shell command upon receiving several of the alerts. In the overall FIPS OS hardening scheme, any possibility of invoking a shell has been eliminated. As a result, this feature is being disabled. The implementation is that upon reconfiguration of alerts (when the user changes the alert and activity configuration and specifies a command to be executed), there will be a check to see if the user has configured any alerts to run a shell command, and if yes this option will not be executed.

The C compiler has been removed so that no one can compile C code. This coupled with the fact that there are no ways of invoking a shell, running an xterm or login to the firewall eliminates the possibility of placing a compiler/source file on the firewall and compiling unauthorized source code.

The /etc/inetd.conf (configuration file for network daemons) has been modified to disable telnet and ftp daemons from running on the firewall. This eliminates the ability to either FTP or telnet to the firewall and further eliminates the possibility of a user using either of these services to access and/or download files to the firewall.

The Remote Web Admin feature has been disabled. This utility allows remote administration of the firewall through Tarantella. The Tarantella based remote web admin is the ability of running telnet daemon on the firewall, which has been disabled through inted.

The Secure Remote Management utility has been disabled. This utility utilizes SSL connections to allow encrypted packets during remote administration of the firewall. The ssh2 component of the firewall, the basis on which this utility works, has been removed from the system to disable this feature.

2.7.3. Procedure for Locking Down the BIOS:

CyberGuard has documented the following procedure for disabling the Floppy and CDROM drives and password protecting the BIOS settings on the box. This will further enhance the hardening of the box so that the drives are under the control of the operator only with the proper password. This will eliminate the possibility of use of any of the two drives to load software by unauthorized access.

2.7.4. To Disable the Floppy drive and the CDROM drive:

When prompted during the initial system boot, press <F2> to enter setup
Select Main
Select Diskette A: [1.44/1.25/1.2 MB 3 ½"] and press <Enter>
Change the Type: field to [None]
Press <Esc>
Select Primary Master [CD-ROM] and press <Enter>
Select Disabled and press <Enter>

2.7.5. To Password Protect the BIOS:

When prompted during the initial system boot, press <F2> to enter setup
Select Security
Select Set Supervisor Password and press <Enter>
Enter New Password xxxxxx
Confirm New Password xxxxxx
Press <Enter>
The Setup Notice message will be displayed
Changes have been saved
Continue

Press <Enter>

Select Exit

Select Exit Saving Changes and press <Enter>

Save configuration changes and exit now? [Yes] <Enter>

3. Cryptographic Key Management

When a Crypto-Officer first creates a CyberGuard Cryptographic Module v5.0P1f profile, DSA signatures are created. CyberGuard Cryptographic Module v5.0P1f users employ these as user authentication during operation. All signatures in the CyberGuard Cryptographic Module v5.0P1f are stored in volatile RAM, and are destroyed (overwritten by zeros) when the Crypto Officer issues a clear command to the module.

When a CyberGuard Cryptographic Module v5.0P1f user receives a challenge, the Diffie-Hellman key agreement process will be involked. The response is transmitted to the creator of the challenge, and the session key is agreed upon. Session keys are destroyed when the session is terminated.

There is no manual key entry is allowed in FIPS mode.

3.1 Cryptographic Algorithms

The following algorithms are incorporated into the CyberGuard Cryptographic Module v5.0P1f.

3.1.1 FIPS Algorithms

1. 3DES-CBC, Encrypt/Decrypt
2. DES-CBC, Encrypt/Decrypt (For legacy systems only)
3. AES-CBC Encrypt/Decrypt
4. SHA-1
5. DSA
6. HMAC-SHA-1

3.1.2 Other Algorithms

7. Diffie-Hellman (Key Agreement)
8. Twofish
9. Blowfish
10. CAST-128
11. Tiger192
12. RipeMD160
13. HMAC-MD5

4. EMI/EMC

Although the CyberGuard Cryptographic Module v5.0P1f consists entirely of software, the FIPS 140-1 tested platform is run on a standard PC, Mac, or Sparc that has been tested for and meets applicable Federal Communication Commission (FCC) Electromagnetic Interference (EMI) and Electromagnetic Compatibility (EMC) requirements for business or home use as defined in Subpart J of FCC Part 15.

The module was tested on an Intel® SR2100/STL2 server (Product Code KB3HSRP) that was EMI/EMC type tested by Intel® to comply to FCC, Part 15 Class A radiated and conducted emissions.

5. Self Tests

The CyberGuard Cryptographic Module v5.0P1f includes several self-tests to ensure the integrity and correct operation of the module. These include the following:

Power-Up Tests	**Name**
Known Hash	SHA-1
Encryption/Decryption	AES
Encryption/Decryption	DES
Encryption/Decryption	3DES
Pairwise consistency	DSA
Software Integrity	HMAC-SHA-1
Conditional Tests	
Random number Generation	ansirand.c
Pairwise consistency	DSA

Table 4: Self-Tests

5.1 Software /Firmware Test

The CyberGuard Cryptographic Module v5.0P1f software module performs a self-integrity check automatically every time it is loaded. The module computes a HMAC-SHA1 MAC over the entire module as per FIPS Pub. 198, and compares the result to a separately stored result. Should the CyberGuard Cryptographic Module v5.0P1f module software be corrupt or been tampered with, the CyberGuard Cryptographic Module v5.0P1f Module Software/firmware Test will fail, alerting the user to the problem and will refuse to load the module.

5.2 Known Answer Tests

The CyberGuard Cryptographic Module v5.0P1f software automatically performs known answer tests of all cryptographic algorithms during module startup as shown in the table above.

5.3 Continuous Random Number Generator Test

The CyberGuard Cryptographic Module v5.0P1f incorporates a Pseudo-random number generator (PRNG) that is compliant with American National Standards Institute (ANSI) X9.31 – 1988 Appendix A.2.4. The PRNG also incorporates a continuous random number generation test, which compares current blocks of data to previous blocks to prevent against failure of the random number generator to a constant value using the tests in the chart above.