GENERAL DYNAMICS
SCOTTSDALE, ARIZONA 85257

GD Crypto Core Shared Library

FIPS 140-2 Non-Proprietary Security Policy

Document Number USD00001070

Document Revision: B

Software Version: 2.1.0

February 07, 2020

REVISION HISTORY

Version	Date	Author	Description
1.0	03/01/2019	Naveed Shah	Initial Release CNs. 1.0 CNUS00045799
2.0	05/01/2019	Naveed Shah	Added HASH_DRBG based on SP 800-90A Rev1 CNs. 2.0 CNUS00008101
–	06/21/2019	Naveed Shah	Updated per Leidos Comments CNs. – CNUS00008791
A	07/09/2019	Naveed Shah	Updated per Leidos Comments CNs. A CNUS00009172
B	02/07/2020	Naveed Shah	Updated per CMVP Comments CNs. B CNUS00013537

TABLE OF CONTENTS

TABLE OF FIGURES

TABLE OF TABLES

1 CRYPTOGRAPHIC MODULE SECURITY POLICY

1.1 Purpose

This is a non-proprietary security policy for the General Dynamics (GD) FIPS 140-2 validated GD Crypto Core Shared Library. The GD Crypto Core Shared Library Security Policy defines the general rules, regulations, and practices under which the GD Crypto Core Shared Library was designed and developed for its correct operation. This Security Policy describes how the GD Crypto Core Shared Library meets the security requirement of Federal Information Processing Standards (FIPS) 140-2.This policy was prepared as part of the Level 1 FIPS 140-2 validation of the module.

Note 1: "Route 66 Cyber" on the cover page is not intended to be interpreted as being part of the GD Crypto Core Shared Library name.

Note 2: "GD Crypto Core Shared Library", "Crypto Core", "GD Crypto Core", "the cryptographic module", and "module" refers to the same module throughout the document.

1.2 References

Table 1-1 provides references used in this document.

Table 1-1: References

Document Number	Document Title	Date
FIPS PUB 140-2	National Institute of Standards and Technology, *Security Requirements for Cryptographic Modules*	May 25, 2001
FIPS 140-2 DTR	National Institute of Standards and Technology, *Derived Test Requirements for FIPS PUB 140-2, Security Requirements for Cryptographic Modules (Draft)*	January 4, 2011
FIPS 140-2 IG	National Institute of Standards and Technology, *Implementation Guidance for FIPS PUB 140-2 and the Cryptographic Module Validation Program*	May 7, 2019
FIPS PUB 198-1	Federal Information Processing Standards Publication, *The Keyed-Hash Message Authentication Code (HMAC)*	July 2008
FIPS PUB 180-4	National Institute of Standards and Technology, *Federal Information Processing Standards Publication, Secure Hash Standard (SHS)*	August 2015
FIPS PUB 197	National Institute of Standards and Technology, *Federal Information Processing Standards Publication 197 Advanced Encryption Standard (AES)*	November 26, 2001
SP 800-38D	Recommendation for Block Cipher Modes of Operation: Galois/Counter Mode (GCM) and GMAC	November 2007
SP 800-90A Rev1	National Institute of Standards and Technology, *NIST Special Publication 800-90A Revision 1*	June 2015

Document Number	Document Title	Date
	Recommendation for Random Number Generation Using Deterministic Random Bit Generators	

1.3 Document Organization

This Route 66 Cyber TM GD Crypto Core Shared Library FIPS 140-2 Non-Proprietary Security Policy is organized as follows:

- Cryptographic Module Security Policy, ***Section 1***
- Operational Environment, ***Section 2***
- Identification and Authentication Policy, ***Section 3***
- Access Control Policy, ***Section 4***
- Key Management, ***Section 5***
- Physical Security Policy, ***Section 6***
- Mitigation of Other Attacks Policy, ***Section 7***
- Self-Tests, ***Section 8***
- Security Rules, ***Section 9***
- User Guidance, ***Section 10***

1.4 Acronyms

Table 1-2 provides a list of acronyms used in this security policy.

Table 1-2: Acronyms

Acronym	Definition
AES	Advanced Encryption Standard
AK	Authentication Key
API	Application Program Interface
CRNGT	Continuous Random Number Generator Test
CSP	Critical Security Parameters
DEK	Data Encryption Key
DEP	Default Entry Point
DRBG	Deterministic Random Bit Generator
FIPS	Federal Information Processing Standards
GCM	Galois Counter Mode
GD	General Dynamics
GPC	General Purpose Computer
HMAC	Hashed Message Authentication Code
IV	Initialization Vector

Acronym	Definition
KAT	Known Answer Test
NDRNG	Non-Deterministic Random Number Generator
OS	Operating System
PUB	Publication
SHA	Secure Hash Algorithm
SP	Special Publication

1.5 GD Crypto Core Specification

The GD Crypto Core is classified as a multi-chip standalone software cryptographic module. The GD Crypto Core is a software shared library that implements FIPS 140-2 approved cryptographic algorithms. The GD Crypto Core provides FIPS 140-2 Level 1 protection.

The GD Crypto Core is a C language shared library which is dynamically linked to the calling application and is loaded into memory for execution by the operating system loader. The GD Crypto Core provides a C language Application Program Interface (API) for use by applications that require authenticated encryption and integrity. The GD Crypto Core includes APIs for the following algorithms:

- AES-256-GCM
- SHA-256

1.5.1 Security Levels

The GD Crypto Core meets the overall requirements applicable to Level 1 security of FIPS 140-2. The categories and the compliance level are listed in ***Table 1-3***.

Table 1-3: GD Crypto Core Security Level Specification

Section	Security Requirement Section	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	1
9	Self-Tests	1
10	Design Assurance	3
11	Mitigation of Other Attacks	N/A

1.5.2 Cryptographic Boundary

The GD Crypto Core is a software cryptographic module. Therefore it does not have any physical components. The GD Crypto Core's physical cryptographic boundary is the enclosure of the General Purpose Computer (GPC) on which it's executing. The GD Crypto Core is entirely contained within the physical cryptographic boundary. The logical cryptographic boundary is around the GD Crypto Core Shared Library. ***Figure 1-1*** illustrates the cryptographic boundaries of the GD Crypto Core Shared Library.

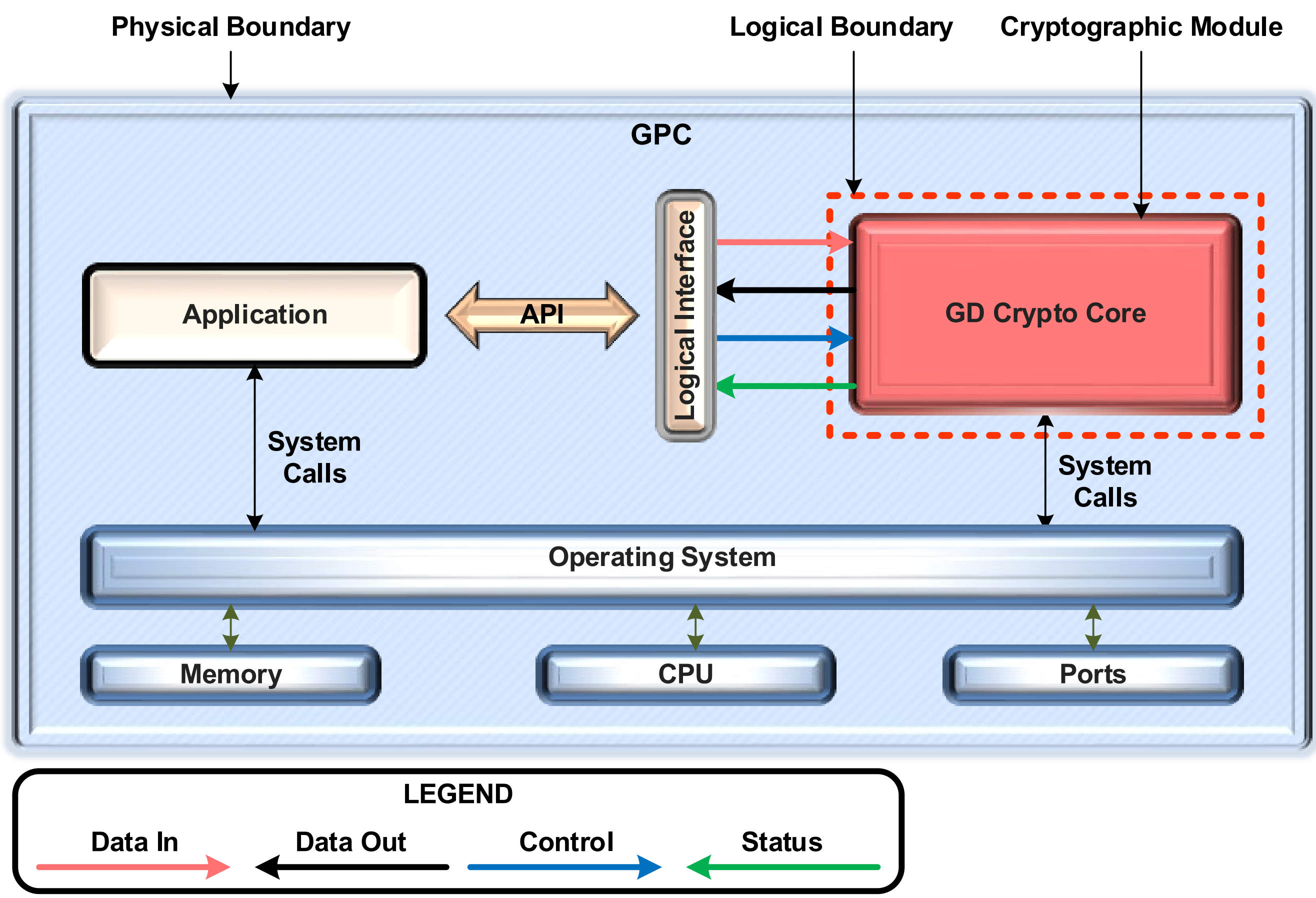

Figure 1-1: GD-Crypto Core Cryptographic Boundary

1.5.3 Ports and Interfaces

The physical ports of the cryptographic module include the ports of the computing platform on which the GD Crypto Core is executed. The physical ports are outside the scope of the FIPS 140-2 validation. The logical interface consists of the C language Application Program Interface (API).

The data input interface consists of the input parameters of the API functions. The data output interface consists of the output parameters of the API. The control interface consists of the API function calls. The status interface is an Error Log API that provides success or failure values to the calling application. Table 1-4 lists the logical interfaces supported by the GD Crypto Core cryptographic module.

Table 1-4: Ports and Interfaces

FIPS 140-2 Logical Interface	Description
Data Input	API input parameters
Data Output	API output parameters
Control Input	API function calls
Status Output	Error Log API (API status parameters)

1.5.4 Modes of Operation

The GD Crypto Core only provides one mode of operation specified as the FIPS Approved Mode of operation. The FIPS Approved Mode of operation is entered by calling the GD_FIPS_mode_set API and upon successfully completion of the power-up self-tests. The GD Crypto Core does not provide a "non-FIPS" mode of operation. The GD Crypto Core does not operate unless FIPS mode is set.

1.5.5 Approved Security Functions

Table 1-5 lists the certificate numbers issued for the approved security functions supported by the GD Crypto Core under the National Institute of Standards and Technology (NIST) Cryptographic Algorithm Validation Program (CAVP). The GD Crypto Core does not implement all of the algorithms/modes (i.e. AES CTR, ECB, and GMAC) verified through the CAVP.

Table 1-5: Approved Security Functions

Security Functions	Certificate Number
Symmetric Algorithm	
➢ AES-256 (FIPS PUB 197) ○ GCM (SP 800-38D)	#C713 and #C714
Secure Hash Standard	
➢ SHA-256 (FIPS PUB 180-4)	#C713 and #C714
Data Authentication Code	
➢ HMAC (FIPS PUB 198-1) ○ (HMAC-SHA-256)	#C713 and #C714
Random Number Generation	
➢ HASH_DRBG SHA-256 (SP 800-90A Rev1)	#C713 and #C714

1.5.6 Non-Approved but Allowed Security Functions

Table 1-6 lists the non-approved but allowed security function used in approved mode of operation.

Table 1-6: Non-Approved but Allowed Security Functions

Security Function	Use
Non-Deterministic Random Number Generator (NDRNG)	An entropy source used for NIST SP 800-90A Rev 1 DRBG.

2 OPERATIONAL ENVIRONMENT

The cryptographic module operates on the General Purpose Computers. The Operating Systems (OS) on the platforms is responsible for providing logical separation. The cryptographic module only allows for single user operation.

2.1 Tested Configurations

The GD Crypto Core has been tested and found to be compliant on the multi-chip standalone platforms listed in ***Table 2-1***.

Table 2-1: Tested Configurations

Operating Systems	Hardware Platform	Processor
Windows 7 (32-bit)	Dell Latitude E6520	Intel® Core™ i7-2640M CPU @ 2.80 GHz
Windows 7 (64 bit)	Dell Latitude E6520	Intel® Core™ i7-2640M CPU @ 2.80 GHz
Windows 10 (64-bit) (32-bit and 64-bit binaries tested)	Dell Latitude E6520	Intel® Core™ i7-2640M CPU @ 2.80 GHz
Red Hat Enterprise Linux 7 (64-bit)	Dell Latitude E6520	Intel® Core™ i7-2640M CPU @ 2.80 GHz
Ubuntu 16.04.4 (64-bit)	Dell Latitude E6520	Intel® Core™ i7-2640M CPU @ 2.80 GHz

2.2 Vendor Affirmed Configurations

Table 2-2 lists the platforms used to test the GD Crypto Core by General Dynamics Mission Systems. GD "vendor affirms" that the GD Crypto Core will operate and provide the same security as on the platforms in the tested configurations. There can be no claim made as to the correct operation of the module or the security strengths of the generated keys when ported to an operational environment which is not listed on the validation certificate.

Table 2-2: Vendor Affirmed Configurations

Operating Systems	Hardware Platform	Processor
Windows 7 (32-bit)	OptiPlex 7020	Intel® Core™ i7-4790

Operating Systems	Hardware Platform	Processor
		CPU @3.60 GHz
Windows 7 (64 bit)	OptiPlex 7010	Intel® Core™ i7-3770 CPU @3.40 GHz
Windows 10 (64-bit)	Latitude 5590	Intel® Core™ i7-8650U CPU @1.90 GHz
Red Hat Enterprise Linux 7 (64-bit)	OptiPlex 5040	Intel® Core™ i7-6700 CPU @3.40 GHz
Ubuntu 16.04.4 (64-bit)	OptiPlex 7020	Intel® Core™ i7-4790 CPU @3.60 GHz

3 IDENTIFICATION AND AUTHENTICATION POLICY

There are two authorized roles that can be assumed by the GD Crypto Core operator. These roles are: User and Cryptographic Officer. These roles are assumed implicitly since the GD Crypto Core does not provide authentication service. The User and Cryptographic Officer roles have access to all Crypto Core Services. As per section 6.1 of the NIST FIPS 140-2 Implementation Guidance, the calling application that loaded the cryptographic module is the operator of the cryptographic module.

4 ACCESS CONTROL POLICY

4.1 Roles and Access to Services

Table 4-1 lists the roles and associated services authorized for each role.

Table 4-1: Services Authorized for Roles

Authorized Services	Roles		Description
	User	Crypto Officer	
Authenticated Encryption	x	x	This service provides 256 bit AES-GCM Encryption of the Plaintext data performed by the GD Crypto Core. ***Input: Data Encryption Key, Plaintext*** ***Output: Initialization Vector, Ciphertext***
Authenticated Decryption	x	x	This service provides 256 bit AES-GCM Decryption of the Ciphertext data performed by the GD Crypto Core. ***Input: Initialization Vector, Data Encryption Key, and Ciphertext*** ***Output: Plaintext***
Message Digest	x	x	This service is used to generate SHA-256 message digest. ***Input: Data*** ***Output: Hash of the Data***
Show Status	x	x	This service provides success or failure code to the calling application. ***Input: N/A*** ***Output: Success or Failure Code***
Perform Self-Tests	x	x	This service performs self-tests upon power-up. ***Input: N/A*** ***Output: Success or Failure Code***

4.2 Services and Access to Keys and CSPs

Table 4-2 also illustrates the access to the keys and the CSPs that is allowable for the GD Crypto Core services. The GD Crypto Core inhibits the output of the encryption keys and the critical security parameters outside of the cryptographic boundary. These are protected within the operating environment.

Table 4-2: Access Rights within Services

Service	Cryptographic Keys and CSPs	Type(s) of Access
Authenticated Encryption	256-bit Data Encryption Key (DEK)	Read, Execute
	Entropy Input	Read, Write, Execute
	Nonce	Read, Write, Execute
	Seed	Read, Write, Execute

Service	Cryptographic Keys and CSPs	Type(s) of Access
	DRBG State Variables (V, C)	Read, Write, Execute
	Initialization Vector	Read, Write, Execute
Authenticated Decryption	256-bit DEK	Read, Execute
	Initialization Vector	Read, Execute
Message Digest	None	N/A
Show Status	None	N/A
Perform Self-Tests	None	N/A

5 KEY MANAGEMENT

Table 5-1 provides a list of keys and CSPs utilized by the GD Crypto Core.

Table 5-1: GD Crypto Core Keys and CSPs

Key/CSP	Use	Generation	Input	Output	Storage	Zeroize
Data Encryption Key (DEK) 256 bits	AES-GCM Encryption/ Decryption	Generated Externally	Memory pointer to a buffer containing the key	N/A	Plaintext in RAM	Zeroized as part of API context cleanup
Authentication Key (AK) 256 bits	A Persistent Key used for Software Integrity Test	Generated Externally	N/A	N/A	Persistent storage in Software Image. Temporary storage in plaintext in RAM.	Not Zeroized
Entropy Input 256 bits	The entropy source to the DRBG	Generated Internally	N/A	N/A	Plaintext in RAM	Zeroize after Use
Nonce 128 bits	Input to DRBG	Generated Internally	N/A	N/A	Plaintext in RAM	Zeroize after Use
Seed 440 bits	Used to instantiate the DRBG	Generated Internally	N/A	N/A	Plaintext in RAM	Zeroize after Use
DRBG State Variables (V, C) 440 bits	DRBG Intermediate Values	Generated Internally	N/A	N/A	Plaintext in RAM	Zeroize after Use

Key/CSP	Use	Generation	Input	Output	Storage	Zeroize
IV 256 bits	AES-GCM Encryption / Decryption	Generated Internally	Memory pointer to a buffer containing the IV	Memory pointer to a buffer containing the IV	Plaintext in RAM	Zeroized as part of API context cleanup

5.1 Key Types

GD Crypto Core supports two keys: Data Encryption Key (DEK) and Authentication Key (AK). The DEK is a 256-bit AES-GCM key which is used for AES-GCM encryption/decryption. The AK is a 256-bit HMAC key which is used in the HMAC SHA-256 calculation which is used for software integrity check of the GD Crypto Core text/data segments.

5.2 Key Generation

GD Crypto Core does not generate keys. The DEK and the AK are generated external to the GD Crypto Core.

5.3 Key Input

GD Crypto Core receives keys in plaintext via a pointer passed by the calling application.

5.4 CSP Output

GD Crypto Core passes the IV via a pointer to the calling application.

5.5 Key/CSP Storage

5.5.1 Persistent Storage

Authentication Key used for software integrity test is stored persistently in the software image.

5.5.2 Non-Persistent Storage

The following Keys/CSPs are stored in RAM:

- Data Encryption Key
- Authentication Key (stored in RAM during software integrity test)
- Entropy Input
- Nonce
- Seed
- DRBG State Variables (V, C)
- Initialization Vector

5.6 Key Zeroization

The keys and CSPs are zeroized as part of the API context cleanup. Memset() function is called to perform zeroization. The only exception is the AK which is not zeroized. The AK is used to check the integrity of the software and must be persistent.

5.7 Random Number Generation

The GD Crypto Core implements a FIPS 140-2 approved hash-based Deterministic Random Bit Generator (DRBG) based on [SP 800-90A Rev 1] to generate an Initialization Vector (IV) for the AES-256-GCM algorithm. The approved DRBG used for random number generation is a HASH_DRBG with derivation function and without prediction resistance. A Non-Deterministic Random Number Generator is used to provide 256 bits of entropy for seeding the DRBG. The DRBG is seeded on every request for a random number for an IV.

6 PHYSICAL SECURITY POLICY

The GD Crypto Core is a software cryptographic module. The physical security requirements are not enforced.

GD Crypto Core is intended to run on a general purpose computing environment that conforms to the EMI/EMC requirements specified by 47 Code of Federal Regulations, Part 15 Subpart B, Unintentional Radiators, Digital Devices, Class A.

7 MITIGATION OF OTHER ATTACKS POLICY

There are no special mechanisms that are built in or designed in the cryptographic module to mitigate specific attacks outside of those required by FIPS 140-2.

8 SELF-TESTS

FIPS 140-2 requires that the cryptographic module perform self-tests to ensure the integrity of the cryptographic module at start up. During the execution of the self-tests, cryptographic services are not available and data input and output is not possible.

8.1 Power-Up Self-Tests (Load Time)

The GD Crypto Core performs power-up self-tests automatically during loading of the GD Crypto Core by making use of a Default Entry Point (DEP) requiring no operator intervention. The availability of the cryptographic module is dependent on the successful completion of power-up self-tests. The enforcement and implementation of the self-test requirements mean that data input, data output, or any cryptographic functions cannot be performed while the cryptographic module is executing self-tests.

On successful completion of the power-up tests, the cryptographic module becomes operational and cryptographic services are available. If any of the self-tests fail, the GD Crypto Core transitions to an error state. Any subsequent calls to the GD Crypto Core will fail and cryptographic operations will not be available.

8.1.1 Software Integrity Test

The integrity of the GD Crypto Core text and data segment is verified using HMAC SHA-256. The digest is computed at build time and stored within the image. The digest is recalculated upon launching of the linking application at OS loader loadtime and compared against the stored digest. If the comparison is successful, then the remaining power-up self-test (consisting of the algorithm-specific Known Answer Test (KAT)) are performed.

8.1.2 Cryptographic Algorithm Tests

Table 8-1 lists the cryptographic algorithm tests that are part of the power-up self-test suite employed by the GD Crypto Core. The cryptographic functions are only available after successful completion of the cryptographic algorithm tests.

Table 8-1: Cryptographic Algorithm Tests

Algorithm	Types of Known Answer Test
AES-256	A Known Answer Test will be performed to check the encrypt implementation of the AES algorithm.
AES-GCM	Known Answer Tests will be performed to check the encrypt and decrypt implementations of the AES GCM algorithm.
SHA-256	A Known Answer Test will be performed to check SHA-256 implementation.
HASH_DRBG	Known Answer Tests for the Health Tests described in SP 800-90A Rev1 for the HASH_DRBG.

8.2 Self-Tests (Run Time)

The self-tests discussed in ***section 8.1*** are performed again at run time prior to GD Crypto Core going operational.

8.3 Conditional Self-Tests

Table 8-2 lists the conditional self-test performed by the GD Crypto Core.

Table 8-2: Conditional Self-Tests

Self-Test	Description
NDRNG Continuous Random Number Generator Test (CRNGT)	A CRNGT is performed each time the GD Crypto Core requests a random number. The CRNGT checks for duplicate contiguous random numbers.
DRBG Continuous Random Number Generator Test (CRNGT)	A CRNGT is performed each time the GD Crypto Core requests a random number. The CRNGT checks for duplicate contiguous random numbers.
HASH_DRBG Health Tests	A Known Answer Test will be performed for the Instantiate and the Generate function every time a random number is

Self-Test	Description
	requested from the DRBG.

8.4 On-Demand Self-Tests

The On-Demand Self-Tests can be initiated by re-loading the module.

9 SECURITY RULES

The design of the GD Crypto Core is constrained by the following security rules which are enforced by the GD Crypto Core to comply with the Level 1 requirements of FIPS 140-2.

9.1 GD Crypto Core Specification Security Rules

Table 9-1 provides security rules for the GD Crypto Core specification.

Table 9-1: GD Crypto Core Specifications Security Rules

Item #	Security Rules
1	The GD Crypto Core shall logically disconnect data output from the processes performing zeroization.
2	The GD Crypto Core shall be able to distinguish between data and control for input and data and status for output.

9.2 Roles and Authentication Security Rules

Table 9-2 provides security rules for the GD Crypto Core roles and authentication.

Table 9-2: Roles and Authentication Security Rules

Item #	Security Rules
1	The GD Crypto Core shall support User and Crypto Officer roles.
2	The GD Crypto Core shall not support concurrent operators.
3	The GD Crypto Core shall not support authentication.

9.3 Key Management Security Rules

Table 9-3 provides security rules for the GD Crypto Core key management.

Table 9-3: Key Management Security Rules

Item #	Security Rules
1	The GD Crypto Core shall not output keys.
2	The CSPs shall be protected against unauthorized disclosure, modification, and substitution.
3	The GD Crypto Core shall provide the ability to zeroize keys.

9.4 Self-Tests Security Rules

Table 9-4 provides security rules for the GD Crypto Core self-tests.

Table 9-4: Self-Tests Security Rules

Item #	Security Rules
1	The GD Crypto Core shall perform software integrity self-test and known answer self-tests on all approved algorithms at power-up.
2	All output data from the GD Crypto Core shall be inhibited when the GD Crypto Core is in an error state or during self-tests.
3	The GD Crypto Core shall implement power-up self-tests that are initiated without operator intervention.
4	The GD Crypto Core shall provide a self-test status indicator.
5	The GD Crypto Core shall enter an error state upon a self-test failure.
6	The GD Crypto Core shall perform DRBG tests as required by NISP SP 800-90A Revision 1.

10 USER AND CRYPTO OFFICER GUIDANCE

General Dynamics will provide the following items to the application vendor:

- “libgdcrypto.so.2.1.0” file for Linux
- “gd-crypto.dll” and “gd-crypto.lib” for Windows
- GD Crypto Core C API document

The vendor will link the GD Crypto Core Shared Library to the application. Upon the first and subsequent instantiation of the host application, at power-up, the GD Crypto Core Shared Library runs the HMAC SHA-256 to validate the integrity of the library by running a load time software integrity test. If successful, the library will perform the rest of the power-up self-tests. If the software integrity test fails, the library will enter an error state. If the first time software integrity test fails, the application vendor should contact General Dynamics.