L3Harris Technologies, Inc.

Harris AES Load Module

Firmware Version: R04A01

FIPS 140-2 Non-Proprietary Security Policy

FIPS Security Level: 1
Document Version: 0.3

Prepared for:

L3HARRIS™

L3Harris Technologies, Inc.
221 Jefferson Ridge Parkway
Lynchburg, VA 24501
United States of America

Phone: +1 434 316-7181
http://www.l3harris.com

Prepared by:

Corsec

Corsec Security, Inc.
13921 Park Center Road, Suite 460
Herndon, VA 20171
United States of America

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

Table of Contents

1 INTRODUCTION 3
1.1 PURPOSE 3
1.2 REFERENCES 3
1.3 DOCUMENT ORGANIZATION 3

2 HALM OVERVIEW 4
2.1 OVERVIEW 4
2.2 MODULE SPECIFICATION 5
2.3 MODULE INTERFACES 7
2.4 ROLES, SERVICES, AND AUTHENTICATION 8
2.4.1 Crypto-Officer Role 8
2.4.2 User Role 9
2.5 PHYSICAL SECURITY 10
2.6 OPERATIONAL ENVIRONMENT 10
2.7 CRYPTOGRAPHIC KEY MANAGEMENT 10
2.8 SELF-TESTS 14
2.9 MITIGATION OF OTHER ATTACKS 14

3 SECURE OPERATION 15
3.1 SECURE MANAGEMENT 15
3.1.1 Initialization 15
3.2 CRYPTO-OFFICER GUIDANCE 15
3.2.1 Management 15
3.2.2 Zeroization 15
3.3 USER GUIDANCE 15

4 ACRONYMS 16

Table of Figures

FIGURE 1 – HALM PORTABLE TERMINALS (LEFT TO RIGHT: 5400, 7200, 7300, AND UNITY) 4
FIGURE 2 – HALM MOBILE TERMINALS (LEFT TO RIGHT: 5300, 7200, 7300, AND UNITY) 4
FIGURE 3 – LOGICAL CRYPTOGRAPHIC BOUNDARY 6
FIGURE 4 – PHYSICAL CRYPTOGRAPHIC BOUNDARY 7

List of Tables

TABLE 1 – SECURITY LEVEL PER FIPS 140-2 SECTION 5
TABLE 2 – FIPS 140-2 LOGICAL INTERFACES 7
TABLE 3 – MAPPING OF CRYPTO-OFFICER ROLE'S SERVICES TO INPUTS, OUTPUTS, CSPS, AND TYPE OF ACCESS 9
TABLE 4 – MAPPING OF USER ROLE'S SERVICES TO INPUTS, OUTPUTS, CSPS, AND TYPE OF ACCESS 9
TABLE 5 – FIPS-APPROVED ALGORITHM IMPLEMENTATIONS 11
TABLE 6 – LIST OF CRYPTOGRAPHIC KEYS AND CSPS 12
TABLE 7 – POWER-UP SELF-TESTS 14
TABLE 8 – ACRONYMS 16

1 Introduction

1.1 Purpose

This is a non-proprietary Cryptographic Module Security Policy for the Harris AES Load Module (HALM) from L3Harris Technologies, Inc. (also referred to as L3Harris throughout this document). This Security Policy describes how the Harris AES Load Module meets the security requirements of FIPS 140-2 and how to run the module in a secure FIPS 140-2 mode. This policy was prepared as part of the Level 1 FIPS 140-2 validation of the module.

FIPS 140-2 (Federal Information Processing Standards Publication 140-2 – *Security Requirements for Cryptographic Modules*) 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 Cryptographic Module Validation Program (CMVP) website, which is maintained by National Institute of Standards and Technology (NIST) and the Canadian Centre for Cyber Security (CCCS): https://csrc.nist.gov/projects/cryptographic-module-validation-program.

The Harris AES Load Module is referred to in this document as the HALM, 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:

- The L3Harris website (www.l3harris.com) contains information on the full line of products from L3Harris.
- The search page on the CMVP website (https://csrc.nist.gov/Projects/cryptographic-module-validation-program/Validated-Modules/Search) can be used to locate and obtain vendor contact information for technical or sales-related questions about 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:

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

This Security Policy and the other validation submission documents were produced by Corsec Security, Inc., under contract with L3Harris. With the exception of this Non-Proprietary Security Policy, the FIPS 140-2 Validation Documentation is proprietary to L3Harris and is releasable only under appropriate non-disclosure agreements. For access to these documents, please contact L3Harris.

2 HALM Overview

2.1 Overview

L3Harris is a leading supplier of systems and equipment for public safety, federal, utility, commercial, and transportation markets. Their products range from the most advanced IP[1] voice and data networks, to industry-leading multiband/multimode radios, and even public safety-grade broadband video and data solutions. Their comprehensive line of software-defined radio products and systems support the critical missions of countless public and private agencies, federal and state agencies, and government, defense, and peacekeeping organizations throughout the world. This Security Policy documents the security features of the Harris AES Load Module (HALM) incorporated into the L3Harris 5300 (Mobile 800Mhz only), 5400 (Portable only), 5500 (Portable only), 7200, 7300, Unity, XG-25P, XG-25M, XG-75 UHF-L, XG-75 VHF, XG-75 (800 MHz) and other terminal products, which are single and multi-band, multi-mode radios that deliver end-to-end encrypted digital voice and data communications, and are Project 25 Phase 2 upgradable[2]. Figure 1 and Figure 2 display some of the many radio terminals the Harris AES Load Module is incorporated into.

Figure 1 – HALM Portable Terminals (Left to Right: 5400, 7200, 7300, and Unity)

Figure 2 – HALM Mobile Terminals (Left to Right: 5300, 7200, 7300, and Unity)

[1] IP – Internet Protocol
[2] Once the Telecommunications Industry Association (TIA) standard is finalized

The terminal products discussed in this Security Policy support FIPS-Approved secure voice and data communication using Advanced Encryption Standard (AES) algorithm encryption/decryption as specified in FIPS 197. The terminal products also ensure data integrity using a Cipher-based Message Authentication Code (CMAC) algorithm as specified in Special Publication 800-38B. The FIPS 140-2 cryptographic module providing the cryptographic services to the terminals is a single firmware component called the Harris AES Load Module. The HALM provides cryptographic services directly to a Digital Signal Processor (DSP) application on Harris terminals.

The Harris AES Load Module is validated at the FIPS 140-2 Section levels shown in Table 1.

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	1
6	Operational Environment	N/A[3]
7	Cryptographic Key Management	1
8	EMI/EMC[4]	1
9	Self-tests	1
10	Design Assurance	1
11	Mitigation of Other Attacks	N/A

2.2 Module Specification

The Harris AES Load Module is a Level 1 firmware module with a multi-chip standalone physical embodiment. The physical cryptographic boundary of the HALM is the outer chassis of the terminal in which it is stored and executed. The logical cryptographic boundary of the Harris AES Load Module is defined by a single executable (HALM_module_R04A01.ess; Firmware Version: R04A01) running on a TI DSP/BIOS[5] 5.33.03 real-time kernel within the L3Harris terminals. See Figure 3 for a depiction.

The module was tested and validated on the L3Harris XG-75P radio. As allowed per FIPS Implementation Guidance section G.5, the vendor affirms the module's continued validation compliance when operating on any of the following platforms:

- 5300 (Mobile 800Mhz only)
- 5400 (Portable only)
- 5500 (Portable only)
- 7200
- 7300
- Unity
- XG-25P

[3] N/A – Not Applicable
[4] EMI/EMC – Electromagnetic Interference / Electromagnetic Compatibility
[5] BIOS – Basic Input Output System

- XG-25M
- XG-75 UHF-L
- XG-75 (800 MHz)

The cryptographic module maintains validation compliance when ported to any other radio platform employing the same operational environment. The CMVP makes no statement as to the correct operation of the module when ported to an operational environment which is not listed on the validation certificate.

The module is entirely encapsulated by the logical cryptographic boundary shown in Figure 3 below. The logical cryptographic boundary of the module is shown with a teal-colored dotted line.

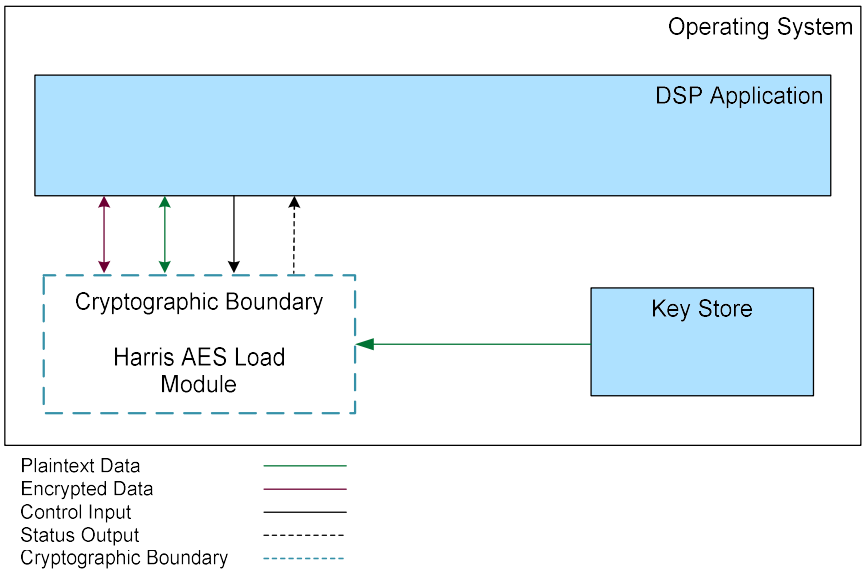

Figure 3 – Logical Cryptographic Boundary

As a firmware cryptographic module, the Harris AES Load Module has a physical cryptographic boundary in addition to its logical cryptographic boundary. The L3Harris terminal hardware that uses the HALM is designed around a Texas Instruments (TI) TMS320C55x device. Each terminal supports a Liquid Crystal Display (LCD), Light Emitting Diode (LED), keypad, speaker, microphone, Universal Device Connector (UDC), and a number of buttons, knobs and switches (as defined in Table 2). The enclosure of the terminal is considered to be the physical cryptographic boundary of the module as shown with a teal-colored dotted line in Figure 4 below.

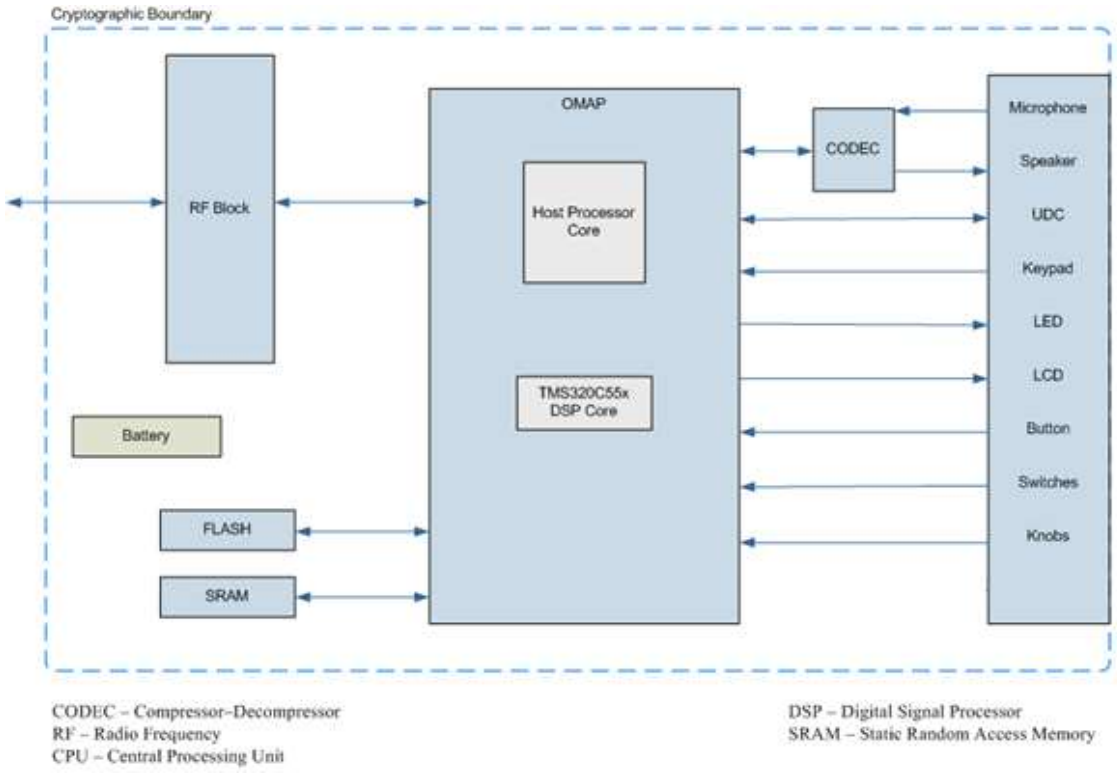

Figure 4 – Physical Cryptographic Boundary

2.3 Module Interfaces

The HALM implements distinct module interfaces in its firmware design. Physically, the module ports and interfaces are considered to be those of the L3Harris terminals on which the firmware executes. However, the firmware communicates through an Application Programming Interface (API), which allows a DSP application to access the executable. Both the APIs and the physical ports in interfaces can be categorized into the 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 module's physical interfaces, as described in Table 2.

Table 2 – FIPS 140-2 Logical Interfaces

FIPS 140-2 Logical Interface	Terminal Physical Port/Interface	Harris AES Load Module Interface
Data Input Interface	• Antenna • Microphone • UDC	Arguments for an API call to be used or processed by the module

FIPS 140-2 Logical Interface	Terminal Physical Port/Interface	Harris AES Load Module Interface
Data Output Interface	• Speaker • Antenna • LCD • LED • UDC	Arguments for an API call that specify where the result of the API call is stored
Control Input Interface	• Keypad • Knobs: Voice Group Selection Knob, Power On-Off/Volume Knob • Buttons: Emergency Button, PTT[6] Button, Option 1 Button, Option 2 Button • A/B Switch • UDC	API call and accompanying arguments used to control the operation of the module
Status Output Interface	• Speaker • Antenna • UDC • LCD • LED	Return values for API calls

2.4 Roles, Services, and Authentication

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. The terminal operator implicitly assumes one of these roles when selecting each command documented in this section.

2.4.1 Crypto-Officer Role

The Crypto-Officer (CO) role is responsible for initializing the module, self-test execution, and status monitoring. Descriptions of the services available to the CO are provided in Table 3 below. Please note that the keys and CSPs listed in the table indicate the type of access required:

- R – Read access: The Critical Security Parameter (CSP) may be read or used within an Approved security function.
- W – Write access: The CSP may be established, generated, modified, or zeroized.

[6] PTT – Push–to–talk

Table 3 – Mapping of Crypto-Officer Role's Services to Inputs, Outputs, CSPs, and Type of Access

Service	Description	Input	Output	CSP and Type of Access
HALM_INITIALIZE	Performs self-tests on demand	API call	Status output	None
HALM_WRAP_KEY	Wraps a key	API call, key, data	Status output, wrapped key	AES Key Wrap Key – R AES Unwrapped Key – R AES Wrapped Key – W
HALM_UNWRAP_KEY	Unwraps a key	API call, key, data	Status output, unwrapped key	AES Key Wrap Key – R AES Wrapped Key – R AES Unwrapped Key – W
HALM_MAC_GENERATION	Generates a Message Authentication Code (MAC)	API call	Status output	AES CMAC key – R
ZEROIZE	Zeroizes keys in volatile memory via power cycle	None	None	AES-256 key – W AES-128 key – W AES CMAC key – W AES Key Wrap Key – W

2.4.2 User Role

The User role has the ability to perform the module's cipher operation, and data or voice conversion services. Descriptions of the services available to the role are provided in Table 4 below. Type of access is defined in section 2.4.1 of this document.

Table 4 – Mapping of User Role's Services to Inputs, Outputs, CSPs, and Type of Access

Service	Description	Input	Output	CSP and Type of Access
HALM_GEN_KEYSTREAM	Generates keystream data	API call	Status output	AES-256 key – R
HALM_GEN_PRIVATE_MI	Generates a Message Indicator (MI) from the Initialization Vector (IV) value specified in the data input buffer	API call	Status output	AES-256 key – R
HALM_P25_XOR	Performs logical exclusive or operation	API call, Plaintext or Ciphertext	Status output, Plaintext or Ciphertext	None
HALM_LOAD_KEY	Load key into the module	API call, key	Status output	AES-256 key – R AES-128 key – R AES CMAC key – R AES Key Wrap Key – R

Service	Description	Input	Output	CSP and Type of Access
HALM_SEND_STATUS	The status of the last functions called from the HALM_API is returned	API call	Status output	None
HALM_AES_OFB	AES OFB Encrypt	API call, key	Status output, encrypted data	AES-256 key – R
HALM_AES_OFB_PASSTHRU	AES OFB Encrypt/Decrypt	Number of iterations; Plaintext or Ciphertext blocks	Plaintext or ciphertext blocks	AES-256 key – R
HALM_AES_ECB	AES ECB Encrypt	API call, key	Status output, encrypted data	AES-256 key – R AES-128 key – R
HALM_AES_ECB_DECRYPT	AES ECB Decrypt	API call, key	Status output, decrypted data	AES-256 key – R AES-128 key – R
HALM_AES_CBC	AES CBC Encrypt	API call, key	Status output, encrypted data	AES-256 key – R
HALM_AES_CMAC	AES CMAC	API call, key	Status output, MAC	AES CMAC key – RX

2.5 Physical Security

The firmware module relies on the physical embodiment of the radios, which store the module within their enclosure. The radios meet Level 1 physical security requirements, and are made of production grade material, opaque within the visible spectrum.

2.6 Operational Environment

Per FIPS Implementation Guidance Section G.3, the operational environment requirements do not apply to the Harris AES Load Module. The cryptographic boundary of the module includes the entire Harris AES Load Module image (HALM_module_R04A01.ess). The firmware image runs on a non-modifiable operational environment, the TI DSP/BIOS 5.33.03 kernel. The kernel does not allow the loading of any new applications. Hence, the operational environment of the module is a non-modifiable operational environment.

2.7 Cryptographic Key Management

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

Table 5 – FIPS-Approved Algorithm Implementations

Cert #	Algorithm	Standard	Modes / Methods	Key Lengths / Curves / Moduli	Use
#2320	AES[7]	FIPS PUB[8] 197 NIST SP 800-38A	CBC[9]	256	Encryption
		NIST SP 800-38B	CMAC[10]	256	Generation/verification *AES CMAC verification is not used by the module*
#2320	AES	FIPS PUB 197 NIST SP 800-38A	ECB[11]	128, 256	Encryption/decryption
		FIPS PUB 197 NIST SP 800-38A	OFB[12]	256	Encryption
#A1249	AES	FIPS PUB 197 NIST SP 800-38F	KW[13]	256	Key wrap/unwrap
#A1249	KTS	NIST SP 800-38F	AES-KW	256	Key transport (key wrapping)

[7] AES – Advanced Encryption Standard
[8] PUB – Publication
[9] CBC – Cipher Block Chaining
[10] CMAC – Cipher-Based Message Authentication Code
[11] ECB – Electronic Code Book
[12] OFB – Output Feedback
[13] KW – Key Wrap

The module supports the critical security parameters listed in Table 6.

Table 6 – List of Cryptographic Keys and CSPs

Key/CSP	Key/CSP Type	Generation / Input	Output	Storage	Zeroization	Use
AES-256 key	256-bit AES key	Generated within the physical boundary; input in plaintext via GPC INT path	Never exits the module	Plaintext in volatile memory	Power cycle zeroizes volatile memory	Used as input into ECB/CBC/OFB cipher operations
AES-128 key	128-bit AES key	Generated within the physical boundary; input in plaintext via GPC INT path	Never exits the module	Plaintext in volatile memory	Power cycle zeroizes volatile memory	Used as input into ECB cipher operations
AES CMAC key	256-bit AES key	Generated within the physical boundary; input in plaintext via GPC INT path	Never exits the module	Plaintext in volatile memory	Power cycle zeroizes volatile memory	Used as input into the CMAC operation
AES Key Wrap Key	256-bit AES Key	Generated within the physical boundary; input in plaintext via GPC INT path	Never exits the module	The key resides in plaintext in volatile memory while in use by the module; The key is not actively stored by the module	Power cycle zeroizes volatile memory	Used as input into the key wrapping and unwrapping operations

Key/CSP	Key/CSP Type	Generation / Input	Output	Storage	Zeroization	Use
AES Wrapped Key	128- or 256-bit AES Key	Generated within the physical boundary; input in wrapped form via GPC INT path	Exits the module in plaintext via GPC INT path	The key resides in plaintext in volatile memory while in use by the module; The key is not actively stored by the module	Power cycle zeroizes volatile memory	The key is passed into the module to be unwrapped by the module and passed back to the terminal
AES Unwrapped Key	128- or 256-bit AES Key	Generated within the physical boundary; input in plaintext via GPC INT path	Exits the module in wrapped form via GPC INT path	The key resides in plaintext in volatile memory while in use by the module; The key is not actively stored by the module	Power cycle zeroizes volatile memory	The key is passed into the module to be wrapped by the module and passed back to the terminal

2.8 Self-Tests

Self-tests are performed by the module once encryption has been activated to check the integrity of the module as well as to ensure the correct performance of AES cryptographic algorithm. The Harris AES Load Module performs the self-tests listed in Table 7 at module startup.

Table 7 – Power-Up Self-Tests

Start-Up Test	Description
Firmware Integrity Test	The module checks the integrity of the binary (using a 256-bit CMAC checksum value) at the start-up. If the MAC verifies correctly (i.e., the newly computed MAC is the same as the stored MAC value), the test passes. Otherwise, it fails.
AES Known Answer Test (KAT)	The AES KAT (128-bit ECB mode) takes a known key and encrypts a known plaintext value. The encrypted value is compared to the expected ciphertext value. If the values differ, the test is failed. The AES KAT then reverses this process by taking the ciphertext value and key; performing decryption; and comparing the result to the known plaintext value. If the values differ, the test is failed. If they are the same, the test is passed.

The module is not required to perform any conditional self-tests as it does not perform the generation of random number or asymmetric key pairs.

The module enters the locked error state if it fails either start-up test. An operator may either restart the terminal, by power cycling the unit or return the terminal to a service depot. The module does not implement any Conditional Self-Test.

2.9 Mitigation of Other Attacks

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

3 Secure Operation

The Harris AES Load Module meets Level 1 requirements for FIPS 140-2. The sections below describe how to place and keep the module in a FIPS-Approved mode of operation.

3.1 Secure Management

The Harris AES Load Module is provided to the Crypto-Officer preloaded in the Harris terminals and is not distributed as a separate executable. The CO does not have to perform any action in order to install or configure the module in the terminals. The HALM, once it is installed, always operates in a FIPS-Approved mode of operation. In order to operate the module, the CO shall turn on the L3Harris terminal.

3.1.1 Initialization

The Harris AES Load Module is initialized by the DSP when the host terminal is powered on. The DSP uses the HALM's initialization routines to load the HALM into memory, allocate memory for operation, and start the module's power-up self-test. Until the module's power-up self-tests have been performed, the module is not operational. The module's services are not available until the module performs and passes its power-up self-test.

3.2 Crypto-Officer Guidance

3.2.1 Management

The Crypto-Officer should monitor the module's status regularly. If any irregular activity is noticed or the module is consistently reporting errors, then L3Harris customer support should be contacted. The operator can determine that the module is operating in the FIPS-Approved mode of operation when the module returns the *HALM_INITIALIZE_OK* status. This status is passed to the operator after the module passes all of its power-up self-tests. The operator can also determine the status of the module by performing the "HALM_SEND_STATUS" service.

3.2.2 Zeroization

The module does not store any keys or CSPs within its logical boundary. All ephemeral keys that are used by the module are zeroized upon shutdown or reboot of the host terminal.

3.3 User Guidance

Users can only access the module's cryptographic functionalities that are available to them. The User should report to the Crypto-Officer if any irregular activity is noticed.

4 Acronyms

This section describes the acronyms.

Table 8 – Acronyms

Acronym	Definition
ADC	Analog to Digital Converter
AES	Advanced Encryption Standard
API	Application Programming Interface
BIOS	Basic Input/Output System
CBC	Cipher Block Chaining
CCCS	Canadian Centre for Cyber Security
CMAC	Cipher-based Message Authentication Code
CMVP	Cryptographic Module Validation Program
CO	Crypto-Officer
CODEC	Compressor-Decompressor
CPLD	Complex Programmable Logic Device
CRC	Cyclical Redundancy Check
CSP	Critical Security Parameter
DAC	Digital to Analog Converter
DSP	Digital Signal Processor
EMC	Electromagnetic Compatibility
EMI	Electromagnetic Interference
FIPS	Federal Information Processing Standard
HALM	Harris AES Load Module
IP	Internet Protocol
IV	Initialization Vector
KAT	Known Answer Test
KTS	Key Transport Scheme
KW	Key Wrap
LCD	Liquid Crystal Display
LED	Light Emitting Diode
MAC	Message Authentication Code
MI	Message Indicator
N/A	Not Applicable
NIST	National Institute of Standards and Technology

Acronym	Definition
OFB	Output Feedback
OMAP	Open Multimedia Application Platform
OS	Operating System
PTT	Push-to-talk
RAM	Random Access Memory
RX	Receive
SRAM	Static Random Access Memory
TI	Texas Instruments
TX	Transmit
UDC	Universal Device Connector

Prepared by:
Corsec Security, Inc.

13921 Park Center Road, Suite 460
Herndon, VA 20171
United States of America

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