

Harris Corporation

Harris AES Software Load Module

Software Version: R04A01

FIPS 140-2 Non-Proprietary Security Policy

FIPS Security Level: I
Document Version: 1.0



Prepared for:



Harris Corporation
1680 University Avenue
Rochester, NY 14610
United States of America

Phone: +1 (585) 244-5830
Email: RFComm@harris.com
<http://www.harris.com>

Prepared by:



Corsec Security, Inc.
13135 Lee Jackson Memorial Hwy., Suite 220
Fairfax, VA 22033
United States of America

Phone: +1 (703) 267-6050
Email: info@corsec.com
<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 AND SERVICES..... | 9 |
| | 2.4.1 <i>Crypto-Officer Role</i> | 9 |
| | 2.4.2 <i>User Role</i> | 9 |
| 2.5 | PHYSICAL SECURITY..... | 10 |
| 2.6 | OPERATIONAL ENVIRONMENT..... | 10 |
| 2.7 | CRYPTOGRAPHIC KEY MANAGEMENT..... | 11 |
| 2.8 | SELF-TESTS..... | 13 |
| 2.9 | MITIGATION OF OTHER ATTACKS..... | 13 |
| 3 | SECURE OPERATION | 14 |
| 3.1 | SECURE MANAGEMENT..... | 14 |
| | 3.1.1 <i>Initialization</i> | 14 |
| | 3.1.2 <i>Management</i> | 14 |
| | 3.1.3 <i>Zeroization</i> | 14 |
| 3.2 | USER GUIDANCE..... | 14 |
| 4 | ACRONYMS | 15 |

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 (PORTABLE TERMINAL)..... | 7 |
| TABLE 3 – FIPS 140-2 LOGICAL INTERFACES (MOBILE TERMINAL)..... | 8 |
| TABLE 4 – MAPPING OF CRYPTO-OFFICER ROLE’S SERVICES TO INPUTS, OUTPUTS, CSPS, AND TYPE OF ACCESS..... | 9 |
| TABLE 5 – MAPPING OF USER ROLE’S SERVICES TO INPUTS, OUTPUTS, CSPS, AND TYPE OF ACCESS..... | 10 |
| TABLE 6 – FIPS-APPROVED ALGORITHM IMPLEMENTATIONS..... | 11 |
| TABLE 7 – LIST OF CRYPTOGRAPHIC KEYS AND CSPS..... | 12 |
| TABLE 8 - LIST OF START-UP SELF-TESTS..... | 13 |
| TABLE 9 – ACRONYMS..... | 15 |



Introduction

1.1 Purpose

This is a non-proprietary Cryptographic Module Security Policy for the Harris AES Software Load Module (HALM) from Harris Corporation. This Security Policy describes how the Harris AES Software 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 Communication Security Establishment Canada (CSEC): <http://csrc.nist.gov/groups/STM/cmvp>.

The Harris AES Software 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 Harris corporate website (<http://www.harris.com>) contains information on the full line of products from Harris.
- The CMVP website (<http://csrc.nist.gov/groups/STM/cmvp/documents/140-1/1401val2011.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:

- 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 Harris. With the exception of this Non-Proprietary Security Policy, the FIPS 140-2 Validation Documentation is proprietary to Harris and is releasable only under appropriate non-disclosure agreements. For access to these documents, please contact Harris.

2 HALM Overview

2.1 Overview

Harris is a leading supplier of systems and equipment for public safety, federal, utility, commercial, and transportation markets. Their products range from the most advanced IP¹ 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 Software Load Module (HALM) incorporated into the Harris 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 upgradable². Figure 1 and Figure 2 display some of the many radio terminals the Harris AES Software 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 software component called the Harris AES Software Load Module. The HALM provides cryptographic services directly to a Digital Signal Processor (DSP) application on Harris terminals.

The Harris AES Software 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 | I |
| 2 | Cryptographic Module Ports and Interfaces | I |
| 3 | Roles, Services, and Authentication | I |
| 4 | Finite State Model | I |
| 5 | Physical Security | N/A |
| 6 | Operational Environment | I |
| 7 | Cryptographic Key Management | I |
| 8 | EMI/EMC ³ | I |
| 9 | Self-tests | I |
| 10 | Design Assurance | I |
| 11 | Mitigation of Other Attacks | N/A |

2.2 Module Specification

The Harris AES Software Load Module is a Level 1 software 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 Software Load Module is defined by a single executable (HALM_module_R04A01.ess; Software Version: R04A01) running on a DSP/BIOS⁴ 5.33.03 software kernel within the Harris terminals. The kernel is a modifiable operational environment since the DSP is also processing instructions supporting the non-security aspects of the terminal. See Figure 3 for a depiction.

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.

³ EMI/EMC – Electromagnetic Interference / Electromagnetic Compatibility

⁴ BIOS – Basic Input Output System

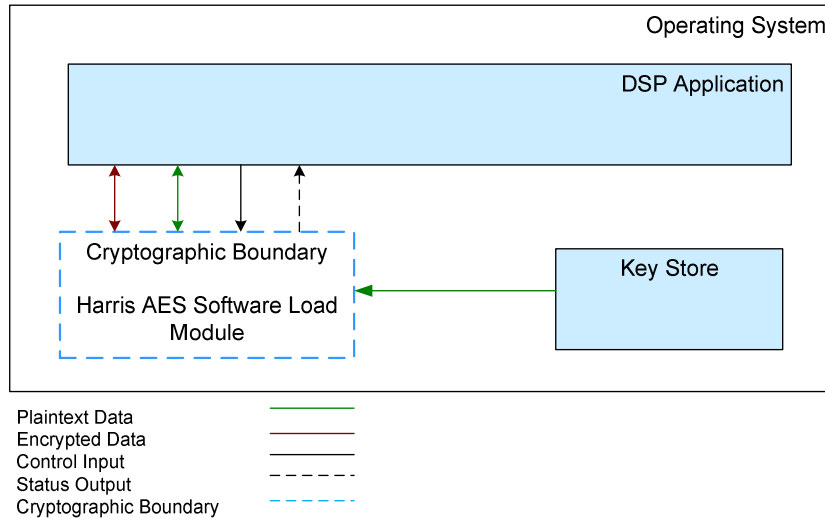


Figure 3 – Logical Cryptographic Boundary

As a software cryptographic module, the Harris AES Software Load Module has a physical cryptographic boundary in addition to its logical cryptographic boundary. The Harris 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 and Table 3). 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.

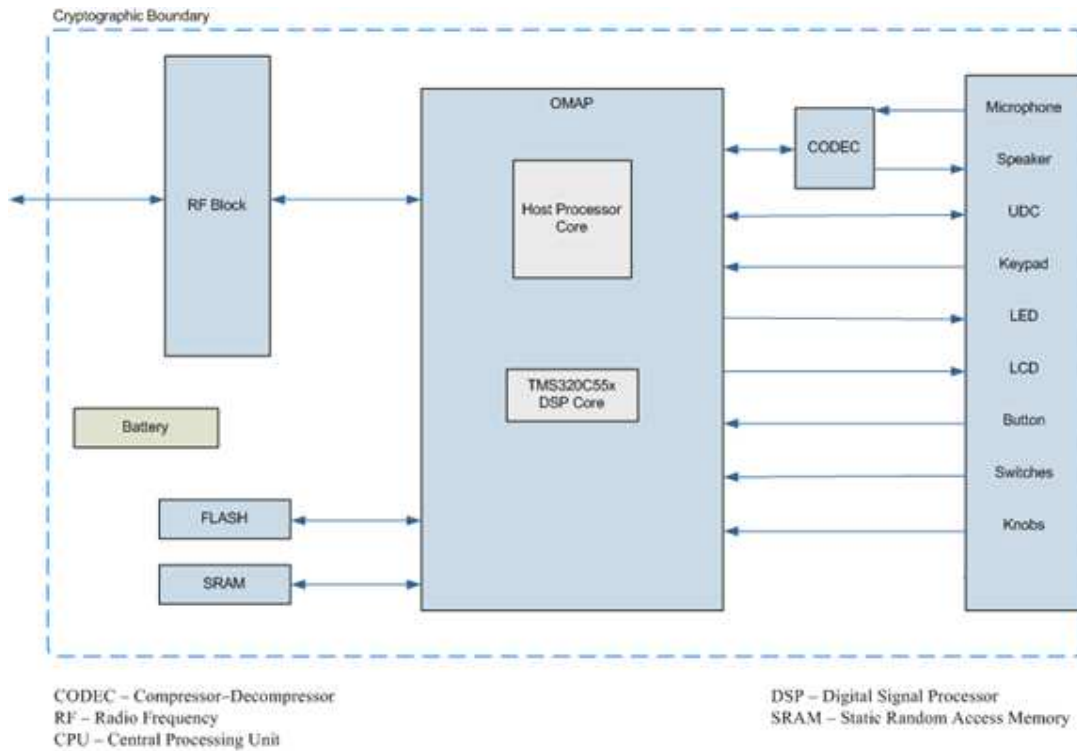


Figure 4 – Physical Cryptographic Boundary

2.3 Module Interfaces

The HALM implements distinct module interfaces in its software design. Physically, the module ports and interfaces are considered to be those of the Harris terminals on which the software executes. However, the software 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 and Table 3.

Table 2 – FIPS 140-2 Logical Interfaces (Portable terminal)

| FIPS 140-2 Logical Interface | Terminal Physical Port/Interface | Harris AES Software Load Module Interface |
|------------------------------|--|---|
| Data Input Interface | <ul style="list-style-type: none"> • 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 Software Load Module Interface |
|------------------------------|---|---|
| Data Output Interface | <ul style="list-style-type: none"> • Speaker • Antenna • LCD • LED • UDC | Arguments for an API call that specify where the result of the API call is stored |
| Control Input Interface | <ul style="list-style-type: none"> • Keypad • Knobs: Voice Group Selection Knob, Power On-Off/Volume Knob • Buttons: Emergency Button, PTT⁵ 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 | <ul style="list-style-type: none"> • Speaker • Antenna • UDC • LCD • LED | Return values for API calls |

Table 3 – FIPS 140-2 Logical Interfaces (Mobile terminal)

| FIPS 140-2 Logical Interface | Terminal Physical Port/Interface | Harris AES Software Load Module Interface |
|------------------------------|--|---|
| Data Input Interface | <ul style="list-style-type: none"> • Antenna Port • GPS Port • Serial Port (DB9) • CAN⁶ Ports (qty 2) • I/O Port (44pin D-sub) | Arguments for an API call to be used or processed by the module |
| Data Output Interface | <ul style="list-style-type: none"> • Antenna Port • Serial Port (DB9) • CAN Ports (qty 2) • I/O Port (44pin D-sub) | Arguments for an API call that specify where the result of the API call is stored |
| Control Input Interface | <ul style="list-style-type: none"> • Antenna Port • Serial Port (DB9) • CAN Ports (qty 2) • I/O Port (44pin D-sub) | API call and accompanying arguments used to control the operation of the module |

⁵ PTT – Push-to-talk⁶ CAN – Controller Area Network

| FIPS 140-2 Logical Interface | Terminal Physical Port/Interface | Harris AES Software Load Module Interface |
|------------------------------|--|---|
| Status Output Interface | <ul style="list-style-type: none"> • Antenna Port • GPS Port • Serial Port (DB9) • CAN Ports (qty 2) • I/O Port (44pin D-sub) | Return values for API calls |

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. 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 4 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.
- W – Write access: The CSP may be established, generated, modified, or zeroized.
- X – Execute access: The CSP may be used within an Approved security function.

Table 4 – 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_UNWRAP_KEY | Unwraps a key | API call, key, data | Status output, key | AES-256 key – X |
| HALM_MAC_GENERATION | Generates a Message Authentication Code (MAC) | API call | Status output | AES-256 key – X |

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 5 below. Type of access is defined in section 2.4.1 of this document.

Table 5 – 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 – X |
| 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 – X |
| 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 |
| HALM_WRAP_KEY | Wraps a key | API call, key | Status output, wrapped key | AES-256 key – X |
| 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 – X |
| HALM_AES_ECB | AES ECB Encrypt | API call, key | Status output, encrypted data | AES-256 key – X AES-128 key – X |
| HALM_AES_ECB_DECRYPT | AES ECB Decrypt | API call, key | Status output, decrypted data | AES-256 key – X AES-128 key – X |
| HALM_AES_CBC | AES CBC Encrypt | API call, key | Status output, encrypted data | AES-256 key – X |
| HALM_AES_CMAC | AES CMAC | API call, key | Status output, MAC | AES-256 key – X |

2.5 Physical Security

The physical security requirements do not apply since the HALM is a software module, which does not implement any physical security mechanisms.

2.6 Operational Environment

The software module was tested and found to be compliant with FIPS 140-2 requirements on the DSP/BIOS 5.33.03 software kernel. The operating system is designed for single user mode and no further action is required to modify the environment for FIPS 140-2 compliance (see Section 3 for guidance).

All cryptographic keys and CSPs are under the control of the OS⁷, 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 AES Cipher-based MAC (CMAC) algorithm.

2.7 Cryptographic Key Management

The module implements the FIPS-Approved algorithms listed in Table 6:

Table 6 – FIPS-Approved Algorithm Implementations

| Algorithm | Certificate Number |
|--|--------------------|
| AES 256-bit encrypt/decrypt in ECB ⁸ and CBC ⁹ modes | 1482 |
| AES 256-bit encrypt in OFB mode | 1482 |
| AES 128-bit in ECB mode | 2320 |
| AES CMAC | 1482 |

The following algorithm is allowed in the FIPS-Approved mode for key wrapping:

- AES (Cert. #1482, key wrapping)

⁷ OS – Operating System

⁸ ECB – Electronic Code Book

⁹ CBC – Cipher Block Chaining

The module supports the critical security parameters listed in Table 7:

Table 7 – 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 Electronically in Plaintext | Never exits the module | Plaintext in volatile memory and flash memory | Power cycle zeroizes volatile memory, key zeroization procedure zeroizes flash memory. | Used as input into the ECB, CBC, and OFB cipher operations. Used for key wrapping |
| AES-128 key | 128-bit AES key | Generated Within the Physical Boundary; Input Electronically in Plaintext | Never exits the module | Plaintext in volatile memory and flash memory | Power cycle zeroizes volatile memory, key zeroization procedure zeroizes flash memory. | Used as input into the ECB cipher operation |

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 Software Load Module performs the self-tests listed in Table 8 at encryption activation

Table 8 - List of Start-up Self-Tests

| Start-Up Test | Description |
|-----------------------------|--|
| AES Known Answer Test (KAT) | The AES KAT 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. |
| Software Integrity Test | The module checks the integrity of the binary (using a 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. |

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.



Secure Operation

The Harris AES Software 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 Software 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 is installed and always operates in a FIPS-Approved mode of operation.

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. However, the operational environment of the module, the DSP/BIOS software kernel, is always in single operator mode by design. Hence, no additional steps are required to fulfill the requirement.

3.1.2 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 Harris customer support should be contacted.

3.1.3 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 reboot or session termination. Outside of the module, external flash memory stores operational keys. These keys are loaded at the point of origin, and may be zeroized by the operator of the radio using the "Key Zero" procedure documented in the terminal's Operator's Manual. After the external flash memory keys are zeroized, the radio must be returned to the point of origin for repair.

3.2 User Guidance

Users can only access the module's cryptographic functionalities that are available to them. 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 describes the acronyms.

Table 9 – 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 |
| 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 |
| CSEC | Communications Security Establishment Canada |
| 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 Software Load Module |
| IP | Internet Protocol |
| IV | Initialization Vector |
| KAT | Known Answer Test |
| LCD | Liquid Crystal Display |
| LED | Light Emitting Diode |
| MAC | Message Authentication Code |
| MI | Message Indicator |
| NIST | National Institute of Standards and Technology |
| OFB | Output Feedback |
| OMAP | Open Multimedia Application Platform |
| OS | Operating System |

| Acronym | Definition |
|----------------|-----------------------------|
| 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.

The logo for Corsec Security, Inc. features the word "Corsec" in a bold, dark red, serif font. The text is centered within a white, three-dimensional oval shape that has a subtle shadow effect, giving it a floating appearance.

13135 Lee Jackson Memorial Hwy., Suite 220
Fairfax, VA 22033
United States of America

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

