Security Policy: Digital Interface Unit Crypto Module (DIU CM)

Version 2.18

7/25/2007

1.0 Introduction

1.1 Scope

This Security Policy specifies the security rules under which the Digital Interface Unit Cryptographic Module, herein identified as the DIU CM, must operate. Included in these rules are those derived from the security requirements of FIPS 140-2 and additionally, those imposed by Motorola. These rules, in total, define the interrelationship between the:

1. module operators,
2. module services,
3. and critical security parameters (CSPs).

1.2 Acronyms

AES	*Advanced Encryption Standard*
CBC	*Cipher Block Chaining*
CFB	*Cipher Feedback*
CKR	*Common Key Reference*
CO	*Crypto Officer*
CSP	*Critical Security Parameter*
DES	*Data Encryption Standard*
DIU CM	*Digital Interface Unit Crypto Module*
ECB	*Electronic Code Book*
HCA	*Home Country Algorithm*
IV	*Initialization Vector*
KEK	*Key Encryption Key*
KID	*Key Identifier*
KLK	*Key Loss Key*
KMM	*Key Management Message*
KPK	*Key Protection Key*
KVL	*Key Variable Loader*
LFSR	*Linear Feedback Shift Register*
MAC	*Message Authentication Code*
MDC	*Motorola Data Communication (signalling protocol used on analog channels)*
OFB	*Output Feedback*
OTAR	*Over-The-Air-Rekeying*
PRNG	*Psuedo Random Number Generator*
RNG	*Random Number Generator*
RSS	*Radio Service Software*
SCI	*Serial Communications Interface*
SPI	*Serial Peripheral Interface*

TEK	*Traffic Encryption Key*

1.3 Overview

The DIU CM provides secure voice and Over-the-Air-Rekeying (OTAR) advanced key management for Motorola's Digital Interface Unit (DIU). The DIU and DIU CM combine to provide these cryptographic services for Motorola's APCO-25 compliant Astro ™ family of console and base station radio infrastructure equipment.

Figure 1 Digital Interface Unit Cryptographic Module

1.4 DIU CM Hardware / Firmware Version Numbers

FIPS Validated Cryptographic Module Hardware Kit Numbers	FIPS Validated Cryptographic Module Firmware Version Numbers
HW P/N T6721A Version CLN7611C	R82.01.02 R82.01.03 R82.01.05

1.5 DIU CM Implementation

The DIU CM is implemented as a multi-chip embedded cryptographic module as defined by FIPS 140-2. It is comprised of the Armor Cryptographic Processor, Flash memory, key zeroization circuitry, tamper circuitry, power regulation, and on board back-up battery all enclosed in tamper protected housing.

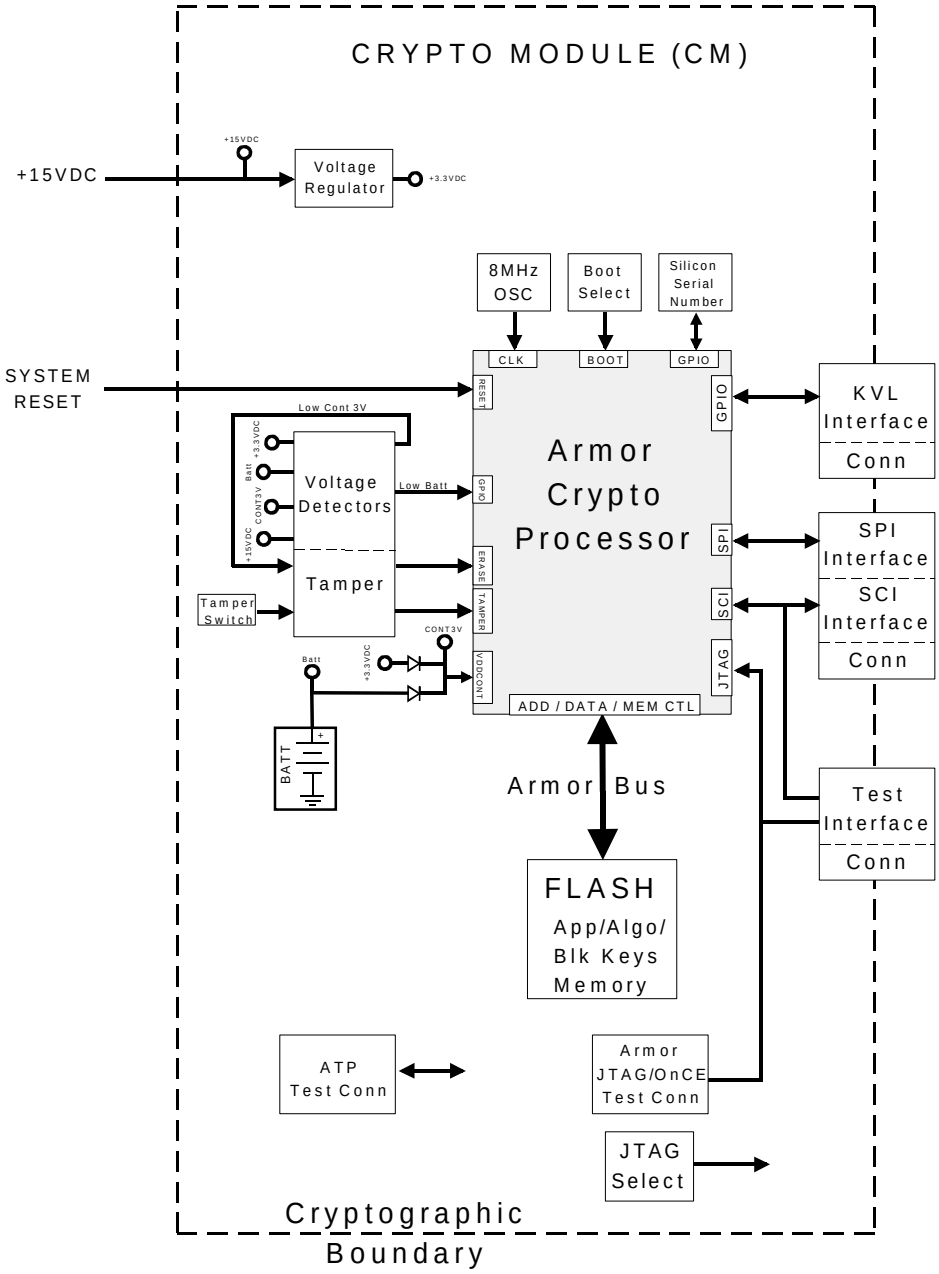
Figure 2 Digital Interface Unit Cryptographic Module (Cover Removed)

1.6 DIU CM Cryptographic Boundary

The DIU CM provides all the cryptographic logic and processes required by the DIU. This includes encryption, decryption, and cryptographic key & critical security parameter storage. The cryptographic boundary is defined as the boundary that encompasses all of the CM circuitry which is bounded by a tamper protected physical enclosure.

The DIU CM consists of the Armor cryptographic processor, flash E^2PROM, SCI port, SPI port, KVL port, Test port, and various support components and circuitry.

Figure 3 DIU CM Cryptographic Boundary



2.0 FIPS 140-2 Security Level

The DIU CM is validated to meet the FIPS 140-2 security requirements for the levels shown in Table 2.1.

Table 2.1
DIU CM Security Levels

FIPS 140-2 Security Requirements Section	Level
Cryptographic Module Specification	1
Cryptographic Module Ports and Interfaces	1
Roles Services and Authentication	2
Finite State Model	1
Physical Security	1
Operational Environment	N/A
Cryptographic Key Management	1
EMI / EMC	1
Self Tests	1
Design Assurance	3
Mitigation of Other Attacks	N/A

3.0 Guidance Documentation

3.1 Administration of the DIU CM in a secure manner (CO)
To install the CM in the DIU in a secure manor, with the DIU powered off, the CM must be placed in the DIU without removing the tamper shield. At initial power up the CM will come up in non-FIPS approved mode. The operator must set FIPS enabled in the Configuration Parameters (via RSS, Radio Service Software) to place the module in FIPS approved mode of operation.

3.2 Assumptions regarding Operator Behavior (CO)
The DIU CM has been designed in such a way that very few assumptions regarding Operator Behavior have been made that are relevant to the secure operation of the module. It has been assumed that the operator will keep all Critical Security Parameters (CSP) private. It has also been assumed that the operator will deny use of the module to unapproved personel while the operator is logged in as the Operator or CO.

3.3 Approved Security Functions, Ports, and Interfaces available to Operators
All DIU CM services are available to the DIU CM operator assuming the appropriate role. These are listed in sections 5-8, 5-10, 5-11 and table 8.3 of this document.

The KVL port and SCI port are directly available to the DIU CM operator. The KVL port is used for electronic key entry and Store & Forward operations. This interface is logically disconnected when the operator is not logged in with the appropriate role. The SCI port is the interface used for the output of plain text digital voice.

3.4 Operator Responsibilities necessary for Secure Operation
The Operator and CO must keep all CSPs private. The Operator and CO must not allow unapproved operation of the module while logged in. The operator must ensure the module is operating in the FIPS approved mode as discussed in section 4 of this document.

4.0 FIPS 140-2 Approved Operational Modes

The DIU CM includes modes of operation that are not FIPS 140-2 approved. Documented below are the configuration settings that are required for the module to be used in a FIPS 140-2 approved mode of operation:
- FIPS mode enabled
- MDC OTAR disabled
- Key Loss Key (KLK) generation disabled
- AES for encryption, decryption, and authentication (authentication, AES MAC, is allowed when used for Project 25 OTAR) shall be used in the following approved modes: ECB, OFB, and CBC
- Use of Triple-DES 8-bit CFB mode for symmetric encryption / decryption of keys and parameters stored in the internal database

The establishment of encryption keys for any of the following non-Approved algorithms will cause the module to enter a non-FIPS approved mode of operation:
- DES (ECB, OFB, CFB, and CBC modes)
- DES-XL
- DVI-XL
- DVP-XL
- ADP
- Home Country Algorithm (HCA)

The operator can use the Key Status service to determine which keys are loaded into the module.

5.0 Security Rules

The DIU CM enforces the following security rules. These rules are separated into two categories, 1) those imposed by FIPS 140-2 and, 2) those imposed by Motorola.

5.1 FIPS 140-2 Related Security Rules

1. The CM supports the following interfaces:
   - Data input interface
     a. Serial Peripheral Interface (SPI) - Bypass Digital Voice, Ciphertext Digital Voice, Key Management Data (OTAR), Encrypted Cryptographic Keys (OTAR), Authentication Data
     b. Serial Communications Interface (SCI) - Plaintext Digital Voice
     c. Key Variable Loader (KVL) - Key Management Data, Encrypted Cryptographic Keys, Plaintext Cryptographic Keys, Encrypted Software Image
     d. Test Port – Factory test
   - Data output interface
     a. Serial Peripheral Interface (SPI) - Bypass Digital Voice, Ciphertext Digital Voice, Key Management Data (OTAR)
     b. Serial Communications Interface (SCI) - Plaintext Digital Voice
     c. Test Port – Factory test
   - Control input interface
     a. Serial Peripheral Interface (SPI) - Input commands
     b. Serial Communications Interface (SCI) - Input commands
     c. Key Variable Loader (KVL) - Input commands
     d. CM System Reset Signal
     e. Test Port – Factory test
   - Status output interface
     a. Serial Peripheral Interface (SPI) - Status codes
     b. Serial Communications Interface (SCI) - Status codes
     c. Key Variable Loader (KVL) - Status codes
     d. Test Port – Factory test
   - Power interface
     a. Power (+15VDC & GND) - Powers all CM circuitry. Internal battery supplies power to battery backed register and tamper detection circuitry when +15VDC not available.
2. The CM inhibits all data output via the data output interface whenever a fatal error state exists and during self-tests.
3. The CM logically disconnects the output data path from the circuitry and processes when performing key generation, manual key establishment, or key zeroization.
4. Plaintext cryptographic keys are entered through the KVL interface only and no plaintext cryptographic keys are ever output from any interface.
5. Authentication data (e.g. passwords) and other critical security parameters are entered in plaintext form and are never output from any interface.
   AND
   plaintext cryptographic keys are entered over a physically separate port.
6. The CM supports an operator role and two categories of cryptographic officer roles. These roles have different sets of services.

7. The CM re-authenticates a role when it is powered-up after being powered-off.
8. The CM provides the following services for the Crypto Officer (Initialization) role:
   - Download Configuration Parameters (CSPs: 40-bit passwords; Algs: n/a)
   - Change password (CSPs: 40-bit passwords; Algs: n/a)
   - Logout (CSPs: none, Algs: n/a)
9. The CM provides the following services for the Crypto Officer (Standard) role:
   - Transfer Unencrypted Key Variables (CSPs: TEK, KEK; Algs: n/a)
   - All services available in the Operator role
10. The CM provides the following services for the Operator role:
    - Privileged APCO OTAR (CSPs: TEK, KEK; Algs: AES)
    - Manual Active Keyset Change (CSPs: none; Algs: n/a)
    - Change Password (CSPs: 40-bit passwords; Algs: n/a)
    - Logout (CSPs: none; Algs: n/a)
    - Encrypt Digital Voice (CSPs: TEK; Algs: AES)
    - Decrypt Digital Voice (CSPs: TEK; Algs: AES)
    - Zeroize Selected Keys (CSPs: TEK, KEK; Algs: n/a)
    - Software Update (CSPs: Plaintext MAC key; Algs: Triple-DES)
11. The CM provides the following services not requiring a role:
    - Login (Validate Password) (CSPs: CO (initialize) password, CO(standard) password, Operator password; Algs: n/a)
    - Software Version/Soundoff/Keep Alive (CSPs: none; Algs: n/a)
    - Initiate Self Tests (CSPs: KPK, TEK; Algs: AES)
    - Zeroize all keys (CSPs: KPK, TEK, KEK, CO (initialize) password, CO(standard) password, Operator password; Algs: n/a)
    - Non-Privileged APCO OTAR (CSPs: none; Algs: n/a)
    - Extract / Clear Error Log (CSPs: none; Algs: n/a)
    - Key Status (CSPs: none; Algs: n/a)
    - Reset Crypto Module (CSPs: none; Algs: n/a)
    - Clear Bypass (CSPs: none; Algs: n/a)
12. The CM enforces Role-Based authentication.
13. The CM implements all software using a high-level language, except the limited use of low-level languages to enhance performance.
14. The CM protects secret keys and private keys from unauthorized disclosure, modification and substitution.
15. The CM provides a means to ensure that a key entered into or stored within the CM is associated with the correct entities to which the key is assigned. Each key in the CM is entered and stored with the following information:
    - Key Identifier – 16 bit identifier
    - Algorithm Identifier – 8 bit identifier
    - Key Type – Traffic Encryption Key or Key Encryption Key
    - Physical ID, Common Key Reference (CKR) number, or CKR/Keyset number – Identifiers indicating storage locations.

    Along with the encrypted key data, this information is stored in a key record that includes a CRC over all of the fields to detect data corruption. When used or deleted the keys are referenced by Key ID/Algid, Physical ID, or CKR/Keyset.

16. The CM denies access to plaintext secret and private keys contained within the CM.
17. The CM provides the capability to zeroize all plaintext cryptographic keys and other unprotected critical security parameters within the CM.
18. The CM supports the following FIPS approved algorithms:
    - Triple-DES
      - 8-bit CFB for symmetric encryption / decryption of keys and parameters stored in the internal database
      - CBC for authentication of software upgrades
      - Triple-DES MAC (vendor affirmed)
    - AES
      - OFB for symmetric encryption / decryption of digital voice and APCO-25 OTAR
      - CBC for authentication of APCO-25 OTAR
      - ECB for symmetric decryption of APCO-25 OTAR
    - SHA-1
      - Password hashing for internal storage
    - ANSI x9.31 PRNG
      - IV and KPK generation
19. The following non-Approved algorithms may be used in the Approved mode of operation:
    - Non-deterministed Hardware RNG
    - LFSR
    - AES MAC for Project 25 OTAR
20. The DIU CM, when used in the DIU, conforms to all FCC Class A requirements.
21. The CM performs the following self-tests:
    - Power-up and on-demand tests
      - Cryptographic algorithm test: Each algorithm (SHA-1, RNG, Triple-DES in the CFB8 and CBC modes, and AES in the OFB, CBC, and ECB modes) is tested by using a known key, known data, and if required a known IV. The data is then encrypted and compared with known encrypted data; the test passes if the final data matches the known data, otherwise it fails. The encrypted data is then decrypted and compared with the original plaintext; the test passes if the final data matches the original data, otherwise it fails.
      - Software/firmware integrity test: The software firmware test calculates a checksum over the code. The checksum is calculated by summing over the code in 32 bit words. The code is appended with a value that makes the checksum value 0. The test passes if the calculated value is 0; otherwise it fails.
      - Clear Bypass test: The output from the module in Clear Bypass mode is redirected to a block of internal RAM. Data is processed using the Clear Bypass mode, and the contents of the RAM block are compared with the data sent. If the contents of the block match the data sent, the test passes, otherwise it fails.

      Powering the module off then on or resetting the module using the CM Reset signal will initiate the power-up and on-demand self tests.
    - Critical Functions tests
      - LFSR Test: The LFSRs are tested by setting the feedback taps to a known value, loading them with known data, shifting the LFSR 64 times, then comparing the LFSR data to a known answer. The test passes if the final data matches, otherwise it fails.

- General Purpose RAM Test: The general purpose RAM is tested for stuck address lines and stuck bits. This is accomplished through a series of operations that write and read the RAM. The test passes if all values read from the RAM are correct; otherwise it fails.

- Conditional tests
  - Software/firmware load test: A MAC is generated over the code when it is built using Triple-DES-CBC. Upon download into the module, the MAC is verified. If the MAC matches the test passes, otherwise it fails.
  - Continuous Random Number Generator test: The continuous random number generator test is performed on 3 Random Number Generators (RNG) within the module. The first is a non-deterministic hardware RNG which is used to seed the ANSI X9.31 deterministic Pseudo Random Number Generator (PRNG) and the maximal length 64-bit LFSR. The second is an implementation of Appendix C ANSI X9.31 which is used for key generation, and the third is a maximal length 64-bit LFSR which is used for IV generation. For each RNG, an initial value is generated and stored upon power up. This value is not used for anything other than to initialize comparison data. A successive call to any one of the RNGs generates a new set of data, which is compared to the comparison data. If a match is detected, this test fails; otherwise the new data is stored as the comparison data and returned to the caller.

22. The CM enters an error state if the Cryptographic Algorithm Test, LFSR Test, Continuous Random Number Generator Test, General-Purpose RAM Test, or the Clear Bypass Test fails. This error state is exited after the CM reset signal is activated or by cycling the power to the CM. The CM performs power-up self tests when its reset signal is activated or its power is cycled. The CM will again enter an error state if these tests continue to fail upon each subsequent power-up self test.
23. The CM enters an error state if the Software/Firmware test fails. This error state is exited after the CM reset signal is activated or by cycling the power to the CM. The CM performs power-up self tests when its reset signal is activated or its power is cycled. The CM will again enter an error state if the Software/Firmware test continues to fail upon each subsequent power-up self test.
24. The CM enters an error state if the Software/Firmware Load test fails. This error state is exited after the CM reset signal is activated or by cycling the power to the CM.
25. The CM outputs an error indication via the status interface whenever an error state is entered due to a failed self-test.
26. The CM does not perform any cryptographic functions while in an error state.

5.2 Motorola Imposed Security Rules

1. The DIU CM does not support multiple concurrent operators.
2. The cryptographic module will continue to provide Operator role and Crypto Officer role services until the module has been powered down or until logged out of the role.
3. All cryptographic module services are suspended during key loading.
4. After more than ten (10) consecutive unsuccessful operator login attempts, the module will zeroize plaintext keys from the key database.
5. Upon detection of a critically low voltage condition on the CM's +15VDC power supply, the cryptographic module shall erase all plaintext keys.

6. Upon detection of a critically low voltage condition on the CM's +3.3VDC internal operating power supply, the cryptographic module shall erase all plaintext keys.
7. Upon detection of a critically low voltage condition on the CM's continuous +3VDC battery backed power supply, the cryptographic module shall erase all critical security parameters (CSPs).
8. Upon detection of tamper, the cryptographic module shall erase all CSPs.
9. The module shall at no time output any CSPs.

6.0 Roles and Services

6.1 DIU CM Supported Roles

The CM supports 3 roles as defined by FIPS 140-2. These roles are defined to be:

- Crypto Officer (Initialization)
- Crypto Officer (Standard)
- Operator role

6.2 DIU CM Services

Services available in Crypto Officer (Initialization) role:

- Download Configuration Parameters: Download configuration parameters used to specify module behavior. Examples include enable/disable FIPS mode, enable/disable KLK generation, password initialization for each role, etc.
- Change Password: Modify the current password used to identify and authenticate the assumed role.
- Logout: Leave the assumed role and deny access to services associated with that role

Services available in Crypto Officer (Standard) role:

- Transfer Unencrypted Key Variables: Transfer key variables to the CM's key database via a Key Variable Loader (KVL).
- All services available in the operator role (see below).

Services available in Operator role:

- Privileged APCO OTAR: Over the Air Rekeying including key modification.
- Manual Active Keyset Change: Modify the currently active keyset used for selecting keys by PID or CKR.
- Change Password: Modify the current password used to identify and authenticate the assumed role.
- Logout: Leave the assumed role and deny access to services associated with that role
- Encrypt Digital Voice: Encrypt digital voice.
- Decrypt Digital Voice: Decrypt digital voice.
- Zeroize Selected Keys: Zeroize selected key variables from the Key Database by Physical ID (PID) or Common Key Reference (CKR).
- Software Update: Update the CM software via the KVL.

Services available without a role:

- Login (Validate Password): Validate the entered password and authenticate the assumed role.

- Software Version/Soundoff/Keep Alive: Provides basic CM keep alive status with simple message response containing version of software currently loaded on CM.
- Initiate Self Tests: Performs module self tests comprised of cryptographic algorithms test, software firmware test, and critical functions test. Initiated by CM reset or transition from power off state to power on state.
- Zeroize All Keys: Zeroize all keys from the Key Database. Available without a Role. (Module can be reinitialized using KVL).
- Non-Privileged APCO OTAR: Over the Air Rekeying excluding KMMs that modify key variables.
- Extract / Clear Error Log: Provides history of error events (Error & software module where occurred) and provides option to clear history of error events.
- Key Status: Provides status of all keys residing in module (Location, ID, algorithm used with).
- Reset Crypto Module: Hardware signal reset of module to remove CM from error states.
- Clear Bypass: Bypass encryption/decryption and allow plaintext to pass through CM.

7.0 Authentication

The DIU CM uses 40-bit passwords, ranging in values from 0 to 1099511627775, to authenticate the Crypto Officer (Initialization) role, the Crypto Officer (Standard) role, and the Operator role. Password attempts are made through the SPI data input interface. The Crypto Officer (Initialization) role password is initialized to a default value during manufacturing. The Crypto Officer (Standard) and Operator role passwords are initialized while in the Crypto Officer (Initialization) role. After authenticating to an individual role, the password for that role may be changed at any time.

More than ten (10) consecutive invalid authentication attempts activates the tamper response; all plaintext keys are zeroized.

8.0 Access Control

Note: The DIU CM does not support public keys.

8.1 Critical Security Parameters (CSPs)

Table 8.1
CSP Definition

CSP Identifier	Description
Key Protection Key (KPK)	Key used to encrypt/decrypt the key database and other non-volatile parameters. It is internally generated and unique each time generated.
Plaintext Traffic Encryption Keys (TEK)	Keys used for voice and Key Management Message (KMM) encryption/decryption.
Plaintext Key Encryption Keys (KEK)	Keys used to encrypt/decrypt keys in OTAR KMMs.
Plaintext MAC Key	Key used for authentication of software upgrade.
Crypto Officer (Initialization) Password	Password entered during operator authentication for the Crypto Officer (Initialization) role.
Crypto Officer (Standard) Password	Password entered during operator authentication for the Crypto Officer (Standard) role.
Operator Password	Operator password entered during operator authentication for the Operator role.

8.2 CSP Access Types

Table 8.2
CSP Access Types

CSP Access Type	Description
Retrieve key	Decrypts encrypted TEKs or KEKs in the database using the KPK and returns plaintext version or returns Software Plaintext MAC Key.
Store key	Encrypts plaintext TEKs or KEKs using the KPK and stores the encrypted version in the database.
Erase Key	Marks encrypted TEK or KEK data in key database as invalid.
Create KPK	Generates and stores new KPK.
Store Password	Hashes operator password and stores it in the database.

8.3 Access Matrix

Table 8.3
CSP versus CSP Access

Operator Service	Retrieve Key	Store Key	Erase Key	Create KPK	Store Password	Crypto Officer (Initialization)	Crypto Officer (Standard)	Operator	No Role Required
1. Download Configuration Parameters (Enable FIPS mode & Initialize CM parameters)					X	X			
2. Transfer Unencrypted Key Variables		X	X				X		
3. Privileged APCO OTAR	X	X	X				X	X	
4, Non Privileged APCO OTAR						X	X	X	X
5. Manual Active Keyset Change							X	X	
6. Change Password					X	X	X	X	
7. Login (Validate Password)						X	X	X	X
8. Logout						X	X	X	
9. Encrypt Digital Voice	X						X	X	
10. Decrypt Digital Voice	X						X	X	
11. Clear Bypass						X	X	X	X
12. Zeroize Selected Keys			X				X	X	
13. Software Version/Soundoff/Keep Alive						X	X	X	X
14. Software Update	X						X	X	
15. Initiate Self Tests				X		X	X	X	X
16. Zeroize All Keys			X			X	X	X	X
17. Extract / Clear Error Log						X	X	X	X
18. Key Status						X	X	X	X
19. Reset Crypto Module						X	X	X	X

9.0 Operational Environment

The DIU CM contains a limited operational environment. This section is therefore not applicable.

10.0 Mitigation of Other Attacks Policy

The DIU CM is not designed to mitigate any specific attacks outside of those required by FIPS 140-2, including but not limited to power consumption, timing, fault induction, or TEMPEST attacks.