Security Policy for the DVP-200

FIPS 140-2 CERTIFICATION DOCUMENT
for
(DVP-200 with Standard Front Panel) 822-2506-002 Rev B / Rev C
(DVP-200 with Night Vision Front Panel) 822-2506-003 Rev B / Rev C
(DVP-200 with Blank Front Panel) 822-2506-004 Rev C / Rev D
(Firmware) 811-4562-004 (Firmware) 811-4563-002

Document Number 964-7935-001
Revision A
CAGE Code 0EFD0

Rockwell Collins

Contract Number None

	NAME	TITLE	APPROVAL
Prepared By:	Forrest J. Leveille	Sr. Software Engineer	N/A
Approved By:	Michael G. Thibault	Sr. Systems Engineer	On File
Approved By:	Chris K. Helfter	Design Assurance Center Engineer	On File

REVISION HISTORY

VER	REV	DESCRIPTION	DATE	APPROVED
-001	-	Initial Release	2015-03-20	Michael G. Thibault
-001	A	ECO-0526671. Changes and clarifications per feedback from the Cryptographic Module Validation Program (CMVP) at the National Institute of Standards and Technology (NIST)	2015-07-20	Michael G. Thibault

Table of Contents

List of Figures

List of Tables

1 DVP-200 Security Policy

Throughout its life cycle, the Rockwell Collins (RC) Data & Voice Privacy Encryption Unit (DVP)-200 will be required to provide an adequate level of protection against modification. This Security Policy outlines the minimum-security requirements and the operational services that support those requirements. The security guidelines, procedures and practices described in this document are to be adhered to by all users with access to the DVP-200.

1.1 DVP-200 Security Level

The cryptographic module meets the overall requirements applicable to FIPS 140-2, Level 1.

Table 1 - Security Requirements

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

1.2 DVP-200 Cryptographic Module

DVP-200 performance is enhanced by the synchronization provisions. The transmitting and receiving units are synchronized by an over-the-air data preamble at the beginning of each transmission. To assure that the synchronization process is highly reliable even in the presence of such disturbances as noise, short fades, and delay distortion, extensive data forward error correction and interleaved coding are used. The result is a probability of synchronization in excess of 99 percent over channels usable for voice communications.

The DVP-200 can be easily integrated into a wide variety of existing voice and data systems. For an analog voice-only application, transmit audio, receive audio, and push-to-talk (key) are the only three signals from the communication system that need to be routed through the DVP-200. With North Atlantic Treaty Organization (NATO) STANAG 4591 Mixed Excitation Linear Predictive enhanced (MELPe) digital voice (included with the DVP-200), an optional data output can be used if the user prefers to bypass the DVP-200 internal data modem. For data rates up to 2400 BPS, data can be sent through the DVP-200

for AES encryption through the DVP-200's internal modem. For data rates up to 19200 BPS, an external modem (such as the Rockwell Collins Q9604) is used after AES encryption by the DVP-200.

Secure data or voice privacy is provided through Advanced Encryption Standard (AES) 128-bit encryption algorithm. This algorithm uses a 128-bit key variable which provides 2^{128} different combinations. Up to eight key variables may be stored in the DVP-200 at one time, allowing flexibility of key management. The multiple key variables may be used for different time periods or for different networks. In addition, the DVP-200 has a proprietary OTAR capability (non-APCO Project 25 compliant) built in so that DVP-200 key sets can be re-keyed remotely (over the air). Public key (PK) allows two DVP-200s to establish a key and communicate with each other without prior agreement of keys.

1.3 Cryptographic Boundary

The DVP-200 is a multi-chip standalone cryptographic module. All cryptographic processing chips are co-located on the Main Processor Board and are contained within an area defined as the cryptographic boundary.

The DVP-200 is made up of four assemblies: the Main Processor Board, the EMI/Power Interface Board, the Display, and the Enclosure. When the EMI/Power Interface Board and the Display are plugged into the Main Processor Board, and fastened into the metal enclosure, a Cryptographic Boundary is established for the complete DVP-200. The DVP-200 Cryptographic Module, in its entirety, is considered to be within the Cryptographic Boundary.

The cryptographic boundary is defined as the entire DVP-200 enclosure. The enclosure contains the Main Processor Board Assembly, the EMI/Power Interface Board, and the Display assembly: there are no exclusions to the cryptographic boundary from these boards. All data signals enter and leave the Main Processor Board using interface connectors J2 and J3, which connect the Main Processor Board to the EMI/Power Interface Board. All inputs, outputs, control, and power feeds enter and leave the DVP-200 via the EMI/Power Interface Board, specifically, its main 55-pin connector P1 and front panel display and buttons. J1 provides power and signaling to the Display. The DVP-200 Display assembly interfaces to the Main Processor Board through connector J1. The Cryptographic Boundary is shown in Figure 1 - DVP-200 Cryptographic Boundary.

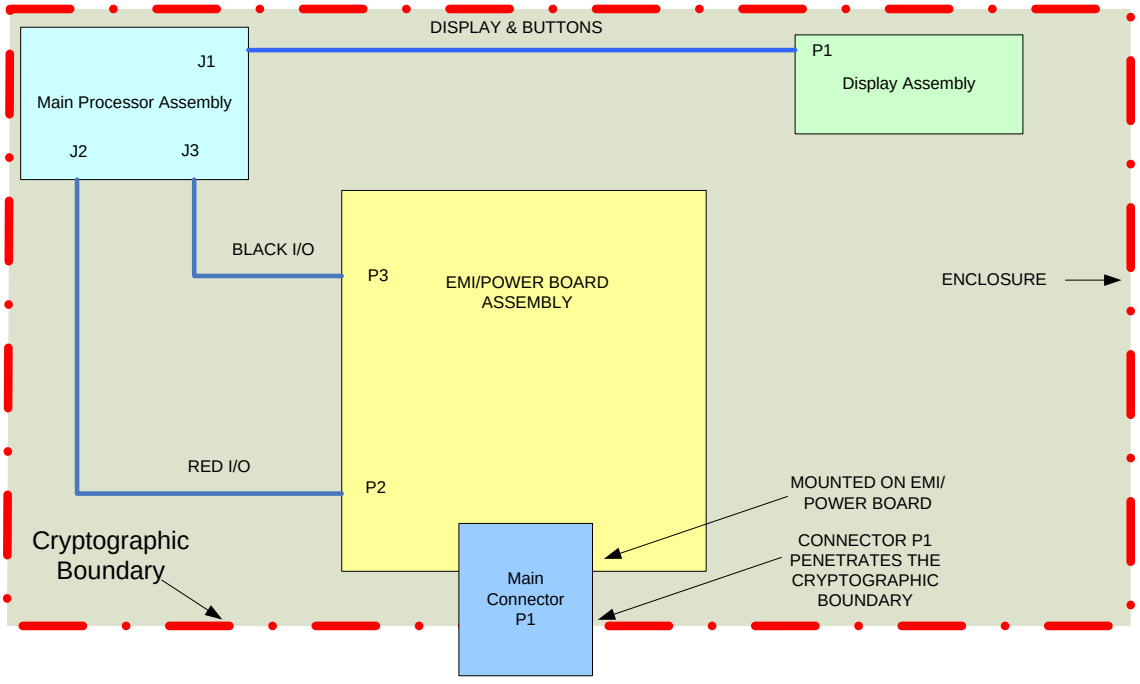

Figure 1 - DVP-200 Cryptographic Boundary

1.4 DVP-200 Overview

The DVP-200 offers a unique combination of data or voice privacy and excellent digital voice quality and is fully compatible with narrowband communications channel including Ultra High Frequency (UHF), Very High Frequency (VHF), High Frequency-Single Sideband (HF-SSB), and telephone.

The DVP-200 is a state-of-the-art version of its predecessor, the VP-116 with data encryption capability and digital voice added. Using a single box (DVP-200), either voice or data encryption (both modes are possible but only one at a time) is accomplished by the DVP-200 simplifying the overall voice and data communications system.

The DVP-200 Cryptographic Modules shown in Figure 2 and Figure 3 illustrates DVPs with front panel interfaces. The front view of the DVP-200 illustrates display and the two push buttons, Mode and Value. The display is a mono-color, four character display with four fasteners for easy panel mounting. The two push buttons are the only operator controls and all features and functions of the DVP-200 can be accessed by sequencing these two buttons. Note that these two models physically look identical to each other when the power is off since the only difference is the Night Vision Front Panel model's backlit LED display intended for use with night vision goggles.

The DVP-200 Cryptographic Module shown in Figure 4 illustrates a DVP with a blank front panel. This model is designed for serial control only for there is no other interface to the DVP such as the push buttons and displays in the other models.

The DVP-200 contains a Main Processor board. The card assembly is approximately 5" x 5" and contains an Analog Devices Blackfin dual-core microprocessor packaged in a 256-pin Ball-Grid-Array, a 16.384 MHz clock oscillator, two independent PIC based Universal Synchronous/Asynchronous Receiver/Transmitter (UART) for the serial ports, an independent UART for set-up, control, and key fill, a watchdog timer, a 16 MegaByte (MB) Synchronous Dynamic Random Access Memory (SDRAM), and 8MB FLASH. There are two versions of the main board which are reflected in the DVP-200 revision letters (e.g., 822-2506-002 Rev B / Rev C). Both boards are electrically equivalent but, in each case, the lower revision letter for the DVP represents a board that has documented factory hand reworks and the higher revision letter for the DVP represents a newer board that has the hand reworks of the lower revision letter incorporated into the board assembly such that there are not any factory hand reworks on the board.

Figure 5 Cryptographic Module Block Diagram depicts the microprocessor data bus and Input/Output destinations. The bus consists of a 32-bit data bus and a 24-bit address bus. The external FLASH hosts the DVP firmware (includes FIPS approved and allowed algorithms), loaded keys, and operator settings. The UART provides capability for Key Fill, configuration, control, zeroization, and status. This path is the only control and status port available due to the legacy terminal design. The terminal device is not part of the FIPS Certification process.

The Advanced Encryption Standard (AES) Crypto-algorithm is run in the Blackfin microprocessor. The Blackfin microprocessor controls loading of the algorithm and handles key management functions for the DVP-200 Cryptographic Module. The Blackfin also collects status information and reports status to the DVP-display and to the terminal device, upon command. The key fill device (terminal device) is an external custom device which interfaces to the DVP-200 through the Receive Exchange Data (RXD) and Transmit Exchange Data (TXD) signals on the P1 connector. Key agreements between two DVP-200s are attainable via the Elliptic Curve Diffie-Hellmann (ECDH) key agreements referred to as a Public Key Exchange (PKE).

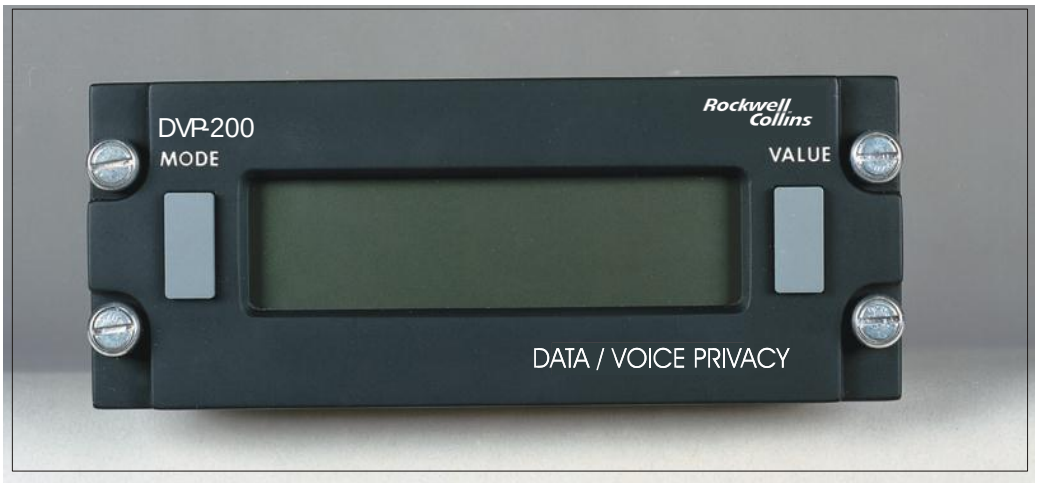

Figure 2 - DVP 200 Standard Front Panel (822-2506-002 Rev B / Rev C) Cryptographic Module

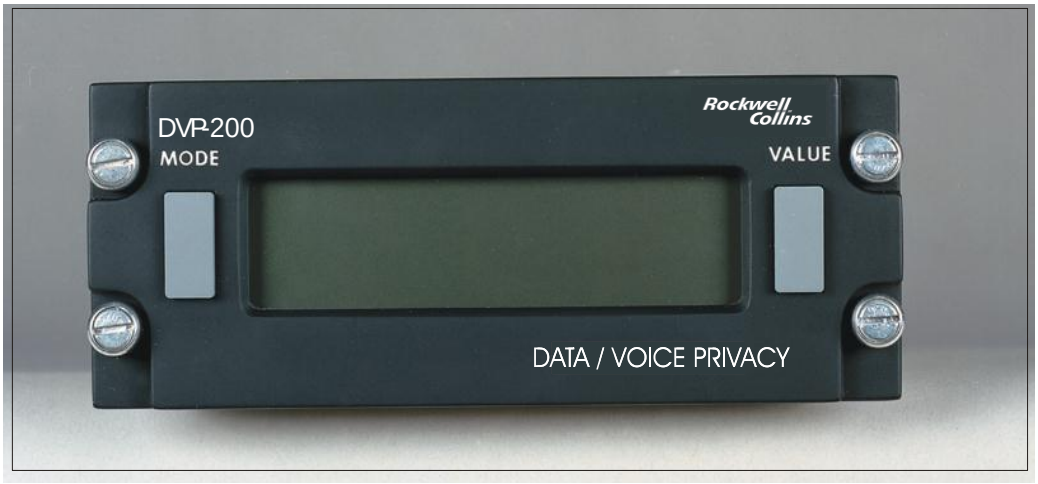

Figure 3 - DVP 200 Night Vision Front Panel (822-2506-003 Rev B / Rev C) Cryptographic Module

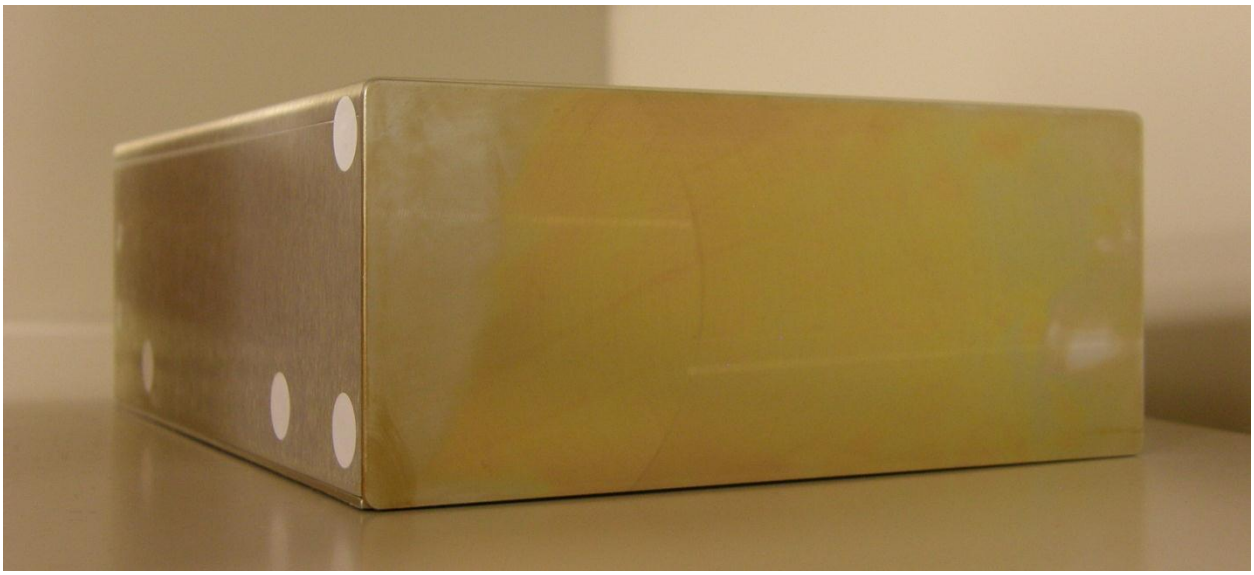

Figure 4 - DVP 200 Blank Front Panel (822-2506-004 Rev C / Rev D) Cryptographic Module

The DVP-200 Block Diagram in Figure 5 illustrates the signal interfaces that are processed by the DVP-200. The processing portion of the DVP-200 is comprised of the Blackfin microprocessor, 16 MB of SDRAM memory, and 8 MB of Flash memory that communicate on common address and data buses. A Temperature Compensated Crystal Oscillator provides the DVP-200 with its clock signals. Two independent PIC microprocessors handle the two serial ports, used for data processing, and route data back and forth to the Blackfin on an independent Serial Peripheral Interface (SPI) bus. Two COder/DECoder (CODEC) devices provide the analog to digital and digital to analog function for the audio signals. External set-up and key loading is performed with an external Terminal Device that interfaces to the DVP-200 via its own Asynchronous serial port. All signals entering and leaving the DVP-200 are buffered. The display and the two control buttons interface directly with the Blackfin microprocessor. The Block Diagram indicates the red/black signal separation and the dedicated signal routing to ensure secure operation. All signals and power are fed through a 55-pin connector that is mounted on the rear apron of the DVP-200 chassis.

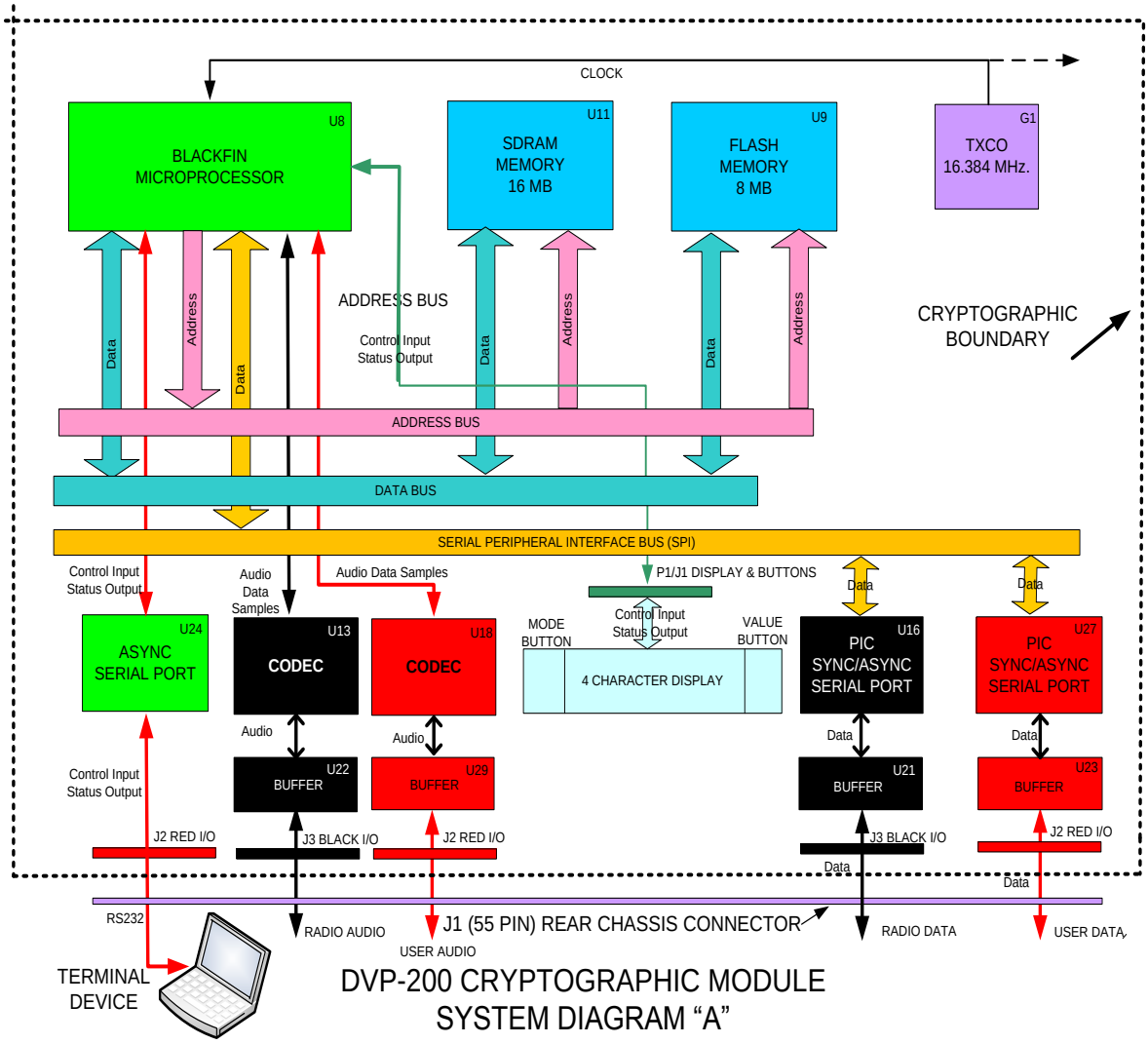

Figure 5 Cryptographic Module Block Diagram

The DVP-200 main board component layout is shown in Figure 5. The three jacks, J1, J2, and J3 provide the signal, power, and display interfaces for the DVP-200. When the Electro-Magnetic Interference (EMI)/Power board and the display module are mated with the main processor board, these three jacks provide the interface. When mated, there is a direct connection between the plugs on the EMI/Power board and the display module and the jacks on the Main Processor board, thus making the interfaces connections completely cable, harness, and wire free. This design provides a high degree of interconnect security since there is no accessible place to probe these interfaces. Since there is a pin-to-pin connection made for each signal and power line, a high degree of reliability is achieved in the DVP-200 design.

The Cryptographic module shall restrict all information flow and physical access points to physical ports and logical interfaces that define all entry and exit points to and from the module. The cryptographic module interfaces shall be logically distinct from each other although they may share one physical port (e.g., input data may enter and output data may exit via the same port) or may be distributed over one or more physical ports (e.g., input data may enter via both a serial and a parallel port). An Application Program Interface (API) of a software component of a cryptographic module may be defined as one or more logical interfaces(s).

The cryptographic module shall have the following four logical interfaces ("input" and "output" are indicated from the perspective of the module):

- *Data input interface*. All data (except control data entered via the control input interface) that is input to and processed by a cryptographic module (including plaintext data, ciphertext data, cryptographic keys and Critical Security Parameters (CSPs), authentication data, and status information from another module) shall enter via the "data input" interface.
- *Data output interface*. All data (except status data output via the status output interface) that is output from a cryptographic module (including plaintext data, ciphertext data, cryptographic keys and CSPs, authentication data, and control information for another module) shall exit via the "data output" interface. All data output via the data output interface shall be inhibited when an error state exists and during self-tests.
- *Control input interface.* All input commands, signals, and control data (including function calls and manual controls such as switches, buttons, and keyboards) used to control the operation of a cryptographic module shall enter via the "control input" interface.
- *Status output interface*. All output signals, indicators, and status data (including return codes and physical indicators such as Light Emitting Diodes and displays) used to indicate the status of a cryptographic module shall exit via the "status output" interface.

All electrical power input to the cryptographic module shall enter via the main connector, J1.

The cryptographic module shall distinguish between data and control for input and data and status for output. All input data entering the cryptographic module via the "data input" interface shall only pass through the input data path. All output data exiting the cryptographic module via the "data output" interface shall only pass through the output data path. The output data path shall be logically disconnected from the circuitry and processes while performing key generation, manual key entry, or key zeroization. To prevent the inadvertent output of sensitive information, two independent internal actions shall be required to output data via any output interface through which plaintext cryptographic keys or CSPs or sensitive data are output (e.g., two different software flags are set, one of which may be user initiated; or two hardware gates are set serially from two separate actions).

Figure 6 illustrates the DVP-200 block diagram and data flow within the DVP-200 and its external ports.

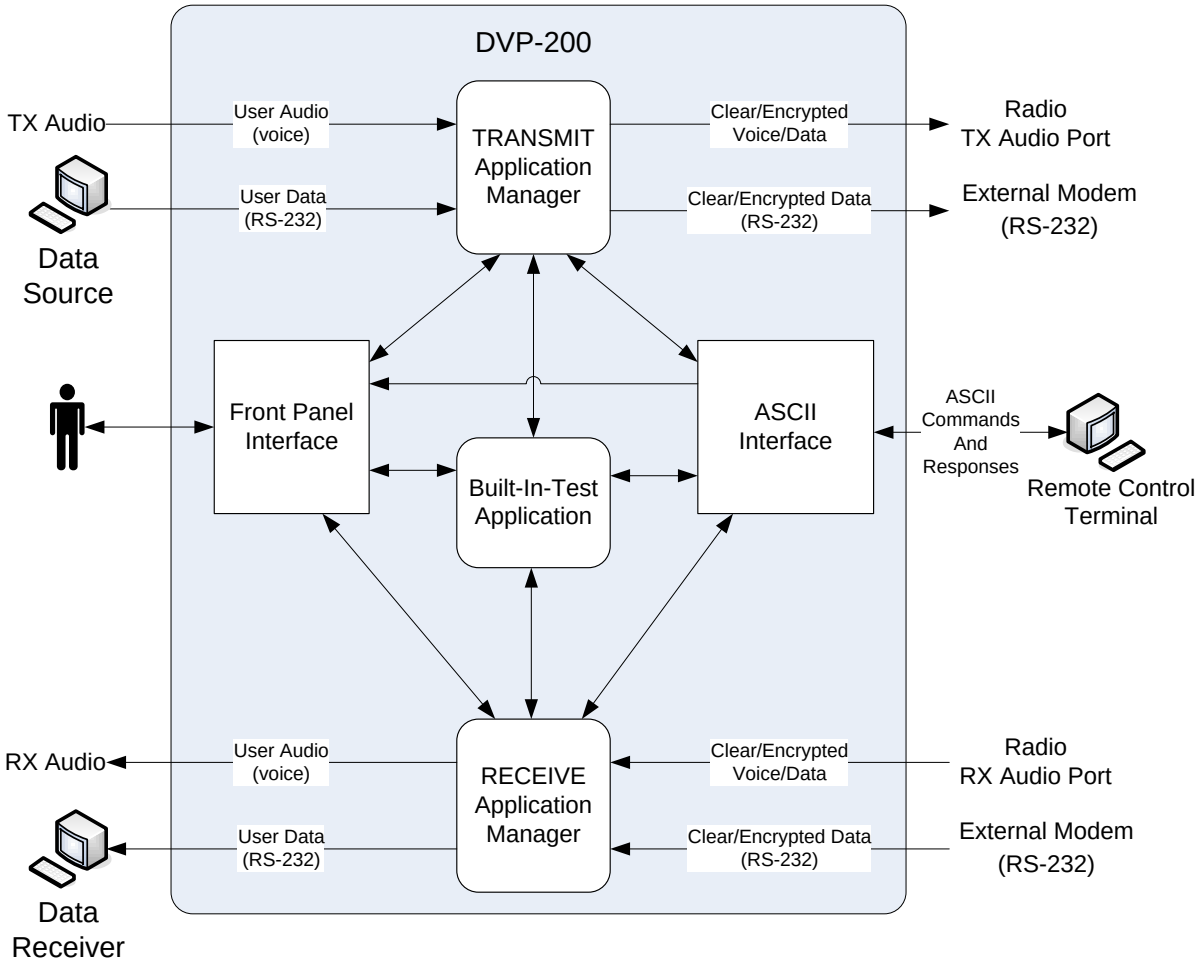

Figure 6 DVP-200 Block Diagram

The DVP-200 is being certified for Security Level 1, and it meets the following basic security requirement:

> For Security Level 1, the physical port(s) and logical interface(s) used for the input and output of plaintext cryptographic keys, cryptographic key components, authentication data, and CSPs may be shared physically and logically with other ports and interfaces of the cryptographic module.

Table 2 - DVP-200 Firmware lists the firmware programmed within the DVP.

Table 2 - DVP-200 Firmware

Collins Part Number	Name	Description
811-4562-004	DVP-200 Blackfin Software	Primary firmware for the DVP-200. Contain all code for the Blackfin microprocessor. This includes user interfaces, digital signal processing, and algorithms that includes AES, RNG, SHA-1, and ECDH.
811-4563-002	DVP-200 PIC Software	Installs in PIC microcontrollers. Provides serial data transfer functionality for DCE and DTE interfaces implemented red and black serial ports. There are not any FIPS algorithms within this item.

Notes:

- The DVP Blackfin Software and the PIC Software are being classified as firmware in the sense that they do not run in a traditional operating system.
- Upon power up, the DVP-200 Blackfin Software is loaded into the Blackfin microprocessor from its nonvolatile flash memory location.
- The DVP does not contain any microcode that Rockwell Collins loads on the Blackfin microprocessor or the PIC microprocessor. These components do contain microcode that is part of the hardware of the two microprocessors.

1.5 Definition of DVP-200 Security Policy

This is the FIPS 140-2 Security Policy for the Rockwell Collins DVP-200. The DVP-200 is intended for airborne, ground, shipboard and ground mobile applications. The DVP-200's function is to encrypt voice and data signals for transmission over narrow-band radio circuits. This Security Policy describes how this module meets the requirements as specified in the Federal Information Processing Standard (FIPS) 140-2 Security Requirements for Cryptographic Modules. Additionally, the Security Policy forms a part of the submission package for the test lab for FIPS Security Level 1 Certification.

1.6 Purpose of DVP-200 Security Policy

FIPS 140-2 specifies the security requirements for a cryptographic module protecting sensitive information. Based on four (4) security levels for cryptographic modules this standard identifies security requirements in eleven sections; Security Policy is one of the sections and this document addresses the design, deployment, and operation of a cryptographic module, providing assurance that the module is properly tested, configured, delivered, installed, and developed, and that the proper operator guidance documentation is provided.

The DVP-200 [CPN 822-2506-002 / -003 / -004] Cryptographic Module is being submitted for FIPS 140-2 Level 1 Security Certification.

2 Reference Documents

Document Number	Title	Date
FIPS 140-2	Security Requirements for Cryptographic Modules	03 Dec 2002
N/A	Implementation Guidance for FIPS PUB 140-2 and the Cryptographic Module Validation Program	02 March 2015
N/A	Derived Test Requirements for FIPS PUB 140-2, Security Requirements for Cryptographic Modules	04 January 2011
670-3524-001 Rev C	Equipment Specification for DVP-200 Data and Voice Privacy Equipment	27 April 2010
964-1751-003 Rev -	DVP-200 Data & Voice Privacy Encryption Unit User's Guide	10 February 2010

3 Specification of the DVP-200 Security Policy

This security policy will put into effect the set of laws, rules, and practices to regulate the management, protection, and distribution of data transmitted over the infrastructure. The policy will apply to users as well as the personnel who maintain and administer the DVP-200. This policy does not replace security requirements of higher organizational level regulations, but is however, the implementation of such requirements.

The DVP-200 should be placed in an environment that enforces safeguarding the DVP against sabotage, tampering, denial of service, espionage, fraud, misappropriation, misuse, or release to unauthorized persons. Continuity of operations is assured for critical functions. The following security policies that apply to DVP-200 include:

- Identification and Authentication
- Access Control
- Physical Security
- Mitigation of other attacks
- Roles, Services and Authentication

3.1 Identification and Authentication Policy

3.1.1 Roles

The DVP-200 will support a Crypto Officer and a User role. The DVP-200 module does not implement authentication. Since the DVP-200 does not implement authentication, the Crypto Officer and User roles are implicitly assumed. A DVP-200 operator may perform both Crypto Officer and User roles if designated to do so. The module does not support a maintenance role. Roles, services, and access to keys and CSPs are summarized in Table 3 - System Roles and Services Matrix.

Table 3 - System Roles and Services Matrix

Service	Cryptographic Key or CSP	Crypto Officer	User	No Role
Power On Self Test	AES Keys ECDH Keys	Execute	Execute	Execute
Built In Test (BIT)	AES Keys ECDH Keys		Execute	
Load AES Keys - Direct	AES Keys	Write		
OTAR Terminal Support Mode	ECDH Keys	Execute		
Initiate OTAR Request	ECDH Keys	Execute		
Acknowledge OTAR Request	ECDH Keys	Execute		
Abort OTAR	AES Keys	Execute		
Load PIN	PIN	Write		
Zeroize	AES Keys ECDH Keys PIN		Execute	
Change Operating Mode	None		Execute	
Select AES Key	AES Keys		Execute	
Initiate a PKE Request	ECDH Keys		Execute	
Acknowledge a PKE Request	ECDH Keys		Execute	
Show Status	None		Read	
Initialize RNG*	RNG Seed RNG Key	Write		Execute
Bypass Includes analog voice, digital voice using MELPe, and data	None		Execute	
Private Includes digital voice using MELPe, and data	AES Keys		Execute	
Factory Reset	All Keys and CSPs	Execute		

* = The initial RNG seed and key are based upon CSPs programmed into the DVP by the Crypto Officer and a random event initiated by the User. After the initial seeding, the RNG is initialized automatically in which the RNG seed and key are based upon stored RNG state values.

3.1.1.1 Crypto Officer Role

The Crypto Officer primary responsibility is to establish each DVP's identity via the UID and PIN and perform key management via a Key Manager personal computer application supplied with a DVP. Key management activities include:

- Generating and loading AES keys
- Generating and loading the DVP PIN
- Generating and loading the DVP UID
- Initiate OTAR requests
- Respond to OTAR requests

By performing any of the above duties, the DVP operator is implicitly acting as a Crypto Officer.

The Key Manager personal computer application includes a database and acts as a Control Terminal to perform the above activities. The computer in which the Key Manager application resides should have user authentication. NOTE: The Key Manager personal computer application is not within the DVP-200 cryptographic module's boundary nor is it considered part of this certification.

3.1.1.1.1 Crypto Officer Guidance

Upon receiving the unit, the Crypto Officer should confirm the unit is a FIPS approved module per Section 3.1.1.3 FIPS Approved Module Confirmation. If the DVP cannot be confirmed to be a FIPS Approved Module, the Crypto Officer should report the findings to the appropriate personnel.

The Crypto Officer should use the Key Manager application supplied with the DVP for managing their DVP Network for it provides the Crypto Officer with means to group various DVPs together and facilitates generating and associating UIDs, PINs, and keys to DVPs. The supplied Key Manager application also provides OTAR capabilities.
Note: The Key Manager application is not within the scope of this certification.

Each DVP should have a unique UID and PIN for OTAR.

If the DVP does not pass BIT, the Crypto Officer should query the unit for its BIT log or BIT report to determine the type of BIT failure. If it a critical security event was triggered (refer to Table 6 – Critical Security Events), the unit may not be usable for some or all secure and nonsecure communications. The Crypto Officer should report the critical security event to the appropriate personnel. If a noncritical security event was triggered, use of the unit may be at the discretion of the Crypto Officer. In either case, critical security event or noncritical security event, the Crypto Officer should attempt to clear the BIT failure by either running BIT and/or cycling DVP power such that PBIT is performed.

If the DVP has remained "ON" for extended periods of time, IBIT should be performed biweekly to verify the unit is functioning properly.

3.1.1.2 User Role

A DVP operator implicitly assumes the User role when operating the DVP and not performing key management or UID, key, or PIN loading..

The activities the User performs are:

- Confirm the unit is a FIPS approved module per Section 3.1.1.3 FIPS Approved Module Confirmation as applicable
  Note: The DVP may be mounted or in a remote location such that it may not be practical to inspect for tampering.

- Controls and operates the DVP. This includes configuring the DVP accordingly to communicate with another User by Clear and/or Private modes of operation in which key selection and participating in PKEs may be required.
  Note: AES keys are loaded prior by the Crypto Officer or are loaded/updated by the OTAR process.
- Performs BIT functions in order to verify the DVP is functioning properly.
- Obtains the Cryptographic Module's status via a Terminal Control device.
- Performs zeroization to zeroize AES and ECDH keys, and the PIN.
- May initiate an OTAR request to update the AES keys
- Controls external equipment associated with the DVP. The equipment may include a radio, modem, data terminal device, and control terminal device.
  Note: A data terminal device sends or receives data transmitted or received by the DVP. A control terminal device is used to control the DVP and/or solicit status.

3.1.1.2.1 User Guidance

Upon receiving the unit, the User should confirm the unit is a FIPS approved module per Section 3.1.1.3 FIPS Approved Module Confirmation. If the DVP cannot be confirmed to be a FIPS Approved Module, the User should report findings to the Crypto Officer or other appropriate personnel.

If the DVP does not pass BIT, the User should query the unit for its BIT log or BIT report to determine the type of BIT failure. If it a critical security event was triggered (refer to Table 6 – Critical Security Events), the unit may not be usable for some or all secure and nonsecure communications. If a noncritical security event was triggered, use of the unit will be at the discretion of the User. In either case, critical security event or noncritical security event, the User should report the event to the Crypto Officer or other appropriate personnel. In addition, the User should attempt to clear the BIT failure by either running BIT and/or cycling DVP power such that PBIT is performed.

If the DVP has remained "ON" for extended periods of time, IBIT should be performed biweekly to verify the unit is functioning properly.

3.1.1.3 FIPS Approved Module Confirmation

The unit should be powered up and verified it passes PBIT. If the unit passes PBIT, the unit is confirmed to be a FIPS Approved Module. If PBIT fails the unit will go to the error state. If the error state is due to a critical security event, the unit will become inoperable. If the unit is not confirmed to be a FIPS Approved Module, the User should report the findings to the appropriate personnel.

3.1.1.4 BIT Faults

If the DVP consistently does not pass BIT, either PBIT or IBIT, the fault should be reported to a designated service depot for instructions on how to proceed.

3.1.2 Authentication Methods and Mechanisms

The DVP-200 module does not implement authentication and is not required for FIPS Security Level 1 Certification.

The Crypto Officer Role primary responsibility is to establish each DVP's identity via the UID and PIN and perform key management via a Key Manager personal computer application supplied with a DVP. Refer to Section 3.1.1.1 Crypto Officer Role for more information.

The User Role is a DVP operator who does not perform key management, key, PIN loading. The User primarily controls the DVP in the field of operation and selects the mode of operation (CLR or PVT) and selects which key index to use for private communications. Refer to 3.1.1.2 User Role for more information.

3.2 Services

This section provides details on the following items:

- All roles supported by a Cryptographic module
- All services provided by a Cryptographic module
- All cryptographic keys and CSPs employed by the Cryptographic Module
- For each role, the services an operator is authorized to perform within that role
- For each service within each role, the type(s) of access to the cryptographic keys and CSPs

3.2.1 Roles

The roles provided by the Cryptographic module are documented in Section 3.1.1 Roles.

3.2.2 Modes of Operation and Algorithms

3.2.2.1 Approved Modes of Operation

FIPS mode is the sole mode of operation for the DVP-200.

The DVP-200 approved algorithms are listed in Table 4 – Security Functions and Approved Algorithms.

Table 4 – Security Functions and Approved Algorithms

Algorithm	Security Function	CAVP Certificate
AES	Output Feedback (OFB) - Data traffic encryption / decryption Electronic Code Book (ECB) - Key validation - PIN validation - OTAR token generation	(ECB (encrypt only[1]; 128); OFB (encrypt/ decrypt; 128)) CAVP Certificate 1504
ANSI X9.62 Random Number Generator (RNG)	- Initialization Vector (IV) for AES OFB mode communications - ECDH	[(P384) (SHA-1)] CAVP Certificate 817
SHA-1	Algorithm used by the RNG	(byte-oriented hashing) CAVP Certificate 1352

[1] Certain data being loaded into the DVP is accompanied with a check word that was generated via ECB encrypt operation. The DVP-200 performs the ECB encrypt operation to the data to derive its check word. If the check word which accompanied the data matched the check word the DVP-200 derived, the data is accepted. As a result, the DVP-200 does not utilize the ECB decrypt operation.

There are no other cryptographic algorithms used on the DVP-200.

Note: For digital voice, the DVP-200 compresses and digitizes voice signals using the MELPe algorithm per STANAG 4591 at 2400 or 1200 bits per second (refer to Table 3 - System Roles and Services Matrix).

3.2.2.1.1 Private Encrypted Mode

Private Encrypted Mode allows for the transmission and reception of data and digital voice encrypted via AES using a 128-bit key. Private Encrypted Mode may be entered via pressing the MODE button on the front panel or by issuing a “PRIV” remote control command. The current status of idle, transmitting, or receiving may be obtained from the remote from issuing the “MODE” command.

3.2.2.1.2 Bypass (Unencrypted) Mode

Bypass (Unencrypted) Mode allows for the transmission and reception of unencrypted data, digital voice, and analog voice. Bypass (Unencrypted) Mode may be entered via pressing the MODE and VALUE buttons on the front panel or by issuing a “CLRA” or “CLRD” remote control command. The current status of idle, transmitting, or receiving may be obtained from the remote from issuing the “MODE” command.

3.2.2.1.3 OTAR Mode

The DVP-200 uses a non-APCO Project 25 compliant OTAR process that includes a message authentication code (MAC) function to remotely rekey a DVP. The module uses ECDH key agreement to provide authentication data during the authentication process and to establish the key used for key wrapping during the rekeying process. This MAC utilizes the DVP's PIN as a key for AES in ECB mode to derive authentication tokens. The tokens are derived from the PIN and part from the ECDH key agreement. Key wrapping utilizes a 128-bit AES key derived from the ECDH key agreement. The key data includes a MAC and is encrypted in with AES in OFB mode.

OTAR Mode allows for the DVP to support OTAR terminal functions or indicates it is in the process of receiving and updating keys remotely via the OTAR process. OTAR Mode for terminal support may only be entered via the "OTAR" remote control command. If the DVP is updating keys from the over-the-air method, the DVP will automatically switch to this mode. Whenever the DVP is in OTAR mode, "OTAR" will be displayed on the front panel. The current status may be obtained from the remote from issuing the "MODE" command.

When a key is accepted via OTAR, "KEY#" is displayed on the front panel where "#" is the AES Key number (between 1 and 8) that was accepted. This allows for a visual status of which key(s) was/were updated.

3.2.2.1.4 Built In Test

Built In Test (BIT) is a superset that includes Power-on BIT (PBIT), Initiated BIT (IBIT), Continuous BIT (CBIT), and Factory BIT (FBIT). These various BITs detect Critical Security Events. There are two levels of Critical Security Events. Table 5 – Critical Security Event Levels defines and describes the Critical Security Event levels. Critical Security events, their levels, and causes are listed in Table 6 – Critical Security Events.

Table 5 – Critical Security Event Levels

Critical Security Event Level	Description
Level 1	The current cryptographic function/process is aborted. This includes: ceasing cryptographic data encryption transmissions, cryptographic data decryption receptions, key agreement establishment, and random number generation. The error is reported and logged. Further Cryptographic functions may be attempted.
Level 2	The highest Critical Security Event level. All of Level 1 Critical Security Events except no security functions are attempted until the error has been cleared. The error may only be cleared by running IBIT or PBIT.

Table 6 – Critical Security Events

Event ID	Critical Security Event Level	Cause
SW_INTEGRITY	Level 2	1. The calculated checksum of the application read from nonvolatile memory did not match the expected value.
BIT_AES	Level 1	1. An error occurred while configuring AES. 2. An error occurred while retrieving a key. 3. An error occurred while verifying a key record. 4. An error occurred during encryption. 5. AES did not encrypt properly (ciphertext output is identical to plaintext input). 6. An error occurred while creating a check word. 7. An error occurred while resetting AES objects.
BIT_RNG	Level 1	1. An error occurred while creating random number generator objects. 2. An error occurred while cycling/seeding the random number generator.
BIT_ECC	Level 1	1. An error occurred while creating PK objects. 2. An error occurred while generating the PK Private and Public keys. 3. An error occurred while generating the PK Shared Secret key
BIT_GENERAL_CRYPTO	Level 1	An error occurred while resetting various cryptographic objects.

3.2.2.1.4.1 PBIT

PBIT is performed automatically when the DVP is powered on.

Table 7 – PBIT Tests

Test	Performed By	Description
Nonvolatile data records	Core B	Performs tests to verify data in non-volatile memory is read correctly
Discrete line	Core B	Performs tests to verify the discrete lines inputs/outputs are functioning correctly.
Internal timers	Core B	Performs checks to verify the internal timers are functioning correctly
PIC Processors	Core B	Performs checks to verify the PIC processors are functioning properly
AES	Core A	Performs select Known Answer Tests (KAT) in ECB mode and a test to verify OFB mode is functioning properly
ECDH PKE	Core A	Performs an internal key agreement
Software Integrity	Core B	Calculates a checksum of the application region of nonvolatile memory and compares it to the expected value.

3.2.2.1.4.2 IBIT

IBIT is initiated at the discretion of the DVP operator (the Crypto Officer or User).

IBIT performs the same tests as PBIT except it does not perform the test to check nonvolatile data records (refer to Table 7 – PBIT Tests).

3.2.2.1.4.3 CBIT

CBIT is performed automatically behind the scenes. It continually monitors the status of functions to determine if a function indicates it has erred or if resulting outputs do not meet specified criteria.

3.2.2.1.4.4 FBIT

FBIT is performed during DVP-200 production to verify the unit meets or exceeds various performance specifications. FBIT requires the DVP to be in a nonstandard configuration that may include various test equipment instrumentation. Table 8 – FBIT Tests lists the items tested during FBIT.

Table 8 – FBIT Tests

Test	Performed By	Description
Watchdog Test	Core B	Verifies the hardware watchdog is functioning properly
FBIT Discrete Tests	Core B	Verifies the Zeroize, PTT, Private Select, Tune In Progress, and Audio Configuration discretes function correctly.
Internal timers	Core B	Performs checks to verify the internal timers are functioning correctly
AES	Core A	Performs select Known Answer Tests (KAT) in ECB mode and a test to verify OFB mode is functioning properly
ECDH PKE	Core A	Performs an internal key agreement
Software Integrity	Core B	Calculates a checksum of the application region of nonvolatile memory and compares it to the expected value.
Tone Test	Core A	Verifies the transmit and receive audio ports are functioning properly.
Nonvolatile data records	Core B	Performs tests to verify data in non-volatile memory is read correctly
PIC Processors	Core B	Performs checks to verify the PIC processors are functioning properly

3.2.2.1.5 Load Keys – Direct

The Crypto Officer may load up to eight AES keys directly into the DVP via a Terminal Device. The command to load keys includes a key index, 1 – 8, the key variable, and a key variable check word. Refer to 3.2.7.1 AES Keys for AES key details.

Loading keys may only be performed anytime the DVP is not busy. Not busy is defined as

- not actively transmitting voice
- not actively transmitting data
- not actively receiving data (receiving digital voice is considered data within the context).

3.2.2.1.6 OTAR Terminal Support Mode

OTAR Terminal Support Mode allows for the DVP to accept OTAR messages to transmit from the OTAR terminal and to send received OTAR messages to the OTAR Terminal. This DVP in OTAR Terminal Support Mode is connected directly to the DVP. The DVP that is the target of an OTAR is considered as a "Remote DVP".

When in OTAR Terminal Support Mode and the OTAR Terminal is not in an active OTAR with another DVP, if the DVP receives a PKE Request, the DVP will forward the request to the OTAR Terminal for it might be a request to OTAR.

The DVP in OTAR Terminal Support Mode performs the following:

- Filters out the Public Key received in a PKE Request and forwards all other PKE Request information to the OTAR Terminal
- Generates the Private and Public Keys and Shared Secret required in the OTAR PKE
- Appends the Public Key to the OTAR PKE Request or Response transmitted
- Forwards the OTAR PKE Shared Secret to the OTAR Terminal so it may be used for Token and Returned Token generation and a portion may be used as the AES key used to encrypt the key structure sent during the OTAR process.
- If in an active OTAR, verifies OTAR information received from other DVPs is from the DVP being OTARed before forwarding the information to the OTAR Terminal

3.2.2.1.7 Initiate OTAR Request

Initiating an OTAR Request may be initiated by the Crypto Officer or User.

3.2.2.1.7.1 Initiate OTAR Request – Crypto Officer

Prior to initiating an OTAR request, the DVP must be placed into OTAR Mode via the Terminal Control which in OTAR terms is referred to as the OTAR Terminal. The OTAR Terminal may then initiate an OTAR request to a designated DVP via the designated DVP's UID. The OTAR request is a normal PKE Requests with the exception of the mode field in the DVP preamble is set to indicate an OTAR PKE Request and the UID is set to the designated UID.

3.2.2.1.7.2 Initiate OTAR Request – User

The User may initiate an OTAR PKE request only by initiating a PKE request. The Crypto Officer must place the Crypto Officer's DVP into OTAR mode via the OTAR Terminal. The Crypto Officer's DVP must be in OTAR mode for it is in this mode that the OTAR Terminal's DVP will forward received the OTAR messages to the OTAR Terminal. When the OTAR Terminal receives a normal PKE Request, the Terminal notifies the Crypto Officer with the sender's UID. The Crypto Officer must accept the request to proceed with the OTAR.

Note: The common practice when a DVP User wants to initiate an OTAR, the User notifies the Crypto Officer in advance. This allows the Crypto Officer to place his DVP in OTAR Support Mode so when the PKE Request is received, the OTAR Terminal receives the request.

3.2.2.1.8 Acknowledge OTAR Request

3.2.2.1.8.1 Acknowledge OTAR Request – Crypto Officer

In the event the User initiated an OTAR request as described in 3.2.2.1.7.1 Initiate OTAR Request – User, the Crypto Officer must accept the request to proceed with the OTAR.

3.2.2.1.8.2 Acknowledge OTAR Request – User

If the User's DVP has a non-zero PIN, the acknowledgment and OTAR process proceeds automatically without User input. If the User's DVP has a zero PIN (a zeroized PIN), the DVP will prompt the User as in a normal PKE Request. If the User acknowledges the request, the OTAR process will proceed.

3.2.2.1.9 Abort OTAR

At any time, the OTAR process may be aborted by either the Crypto Officer or User.

3.2.2.1.9.1 Abort OTAR – Crypto Officer

An OTAR may be aborted anytime by the Crypto Officer by performing any of the following:

- Changing the DVP mode
- Issue a new OTAR command

3.2.2.1.9.2 Abort OTAR – User

An OTAR may be aborted anytime by the User by performing any of the following:

- Changing the DVP mode
- Enable PTT
- Enable a data transmission

3.2.2.1.10 Load PIN

The Crypto Officer may load a PIN via a Terminal Device. The command to load keys includes the PIN and an optional check word. The PIN check word is identical to an AES Key Check Word except the PIN is encrypted to generate the Check Word instead of an AES Key (refer to 3.2.7.1.3 Key Check Word).

3.2.2.1.11 Zeroize

Zeroization may be initiated by one of four methods:

- Discrete Line
- Front Panel
- Terminal Control
- Factory Reset

Zeroization consists of zeroizing or erasing all storage locations for RNG Seed, RNG Key, AES Keys, ECDH Keys, and PIN.

3.2.2.1.12 Change Operating Mode

The operating mode may be changed via front panel or Terminal Control.

3.2.2.1.13 Select AES Key

Selecting a key may be done via the front panel or Terminal Control. When selecting a key with the front panel, the DVP must be in PVT mode.

3.2.2.1.14 Initiate a PKE Request

Initiating a PKE Request may be done via the front panel or Terminal Control.

3.2.2.1.15 Acknowledge a PKE Request

Acknowledging a PKE Request may be done via the front panel or Terminal Control.

3.2.2.2 Non-approved Modes of Operation

There are no non-approved modes of operation used on the DVP-200.

3.2.2.3 Other Algorithms

The DVP-200 allowed or non-FIPS approved algorithms and protocols are listed in Table 9 – Other Algorithms.

Table 9 – Other Algorithms

Algorithm/Protocol	Used for
Elliptic Curve Diffie-Hellman (ECDH)	- Key agreement via DVP's Public Key (PK) mode - Key agreement for key wrapping used for proprietary DVP OTAR Note: ECDH uses a NIST recommended P384 curve and provides 192 bits of encryption strength. Allowed for FIPS mode key establishment.
AES Key Wrapping (AES Cert. #1504)	Over-The-Air-Rekeying (OTAR) of the module. Key wrapping provides 128 bits of encryption strength. (ECDH used for key establishment method. Allowed for FIPS mode encrypted key entry.)
AES MAC (AES Cert. #1504)	- Authenticating key source and target unit during OTAR. - Authenticating the key received during OTAR. (Allowed for FIPS mode message authentication.)

3.2.3 Access Control Configuration

The module is designed to detect unauthorized modification of cryptographic software and firmware by an integrity test.

3.2.3.1 Execution of Cryptographic Features

Execution of stored cryptographic software and firmware features is not prevented except on detection of the following events:

- Zeroization
- Key loading
- Voltage transient conditions
- Internal stored key is not validated due to an incorrect check word or checksum,
- Hash code of the crypto algorithm memory is invalidated
- Cryptographic errors are detected during a cryptographic activity

3.2.3.2 Modification Roles

Restrictions and roles assigned to modification (i.e. write, replace, and delete) of these cryptographic module software or firmware components stored within the cryptographic boundary.

3.2.3.2.1 Cryptographic Programs

The cryptographic programs are not modifiable or erasable.

3.2.3.2.2 Cryptographic Data

Cryptographic data to include keys are modifiable by approved Cryptographic Officer with compatible cryptographic key loader and software with the exception of zeroization where zeroization may be performed by either the Cryptographic Officer or User.

3.2.3.2.3 Critical Security Parameters

Critical Security Parameters are not modifiable or erasable in the Blackfin-based Cryptographic Module.

3.2.3.2.4 Plaintext Data

Plaintext Data is not modifiable by operator or operator system.

The cryptographic operator is able to command deletion of plaintext data.

The cryptographic module is capable of deletion of plaintext data upon receipt of operator command, or voltage out of range detection and a software command.

3.2.3.3 Reading Cryptographic Data

Reading of cryptographic data, critical security parameters and plaintext data is not allowed by the DVP-200 cryptographic module or its operating system. Once the module is sealed with the tamper evident tapes, no external mechanism exists to allow external access to the software.

3.2.3.4 Entering Cryptographic Data

Critical Security Parameters form a part of the delivered cryptographic module and not enterable by the operation system or operator.

Cryptographic Data (e.g. cryptographic keys) is allowed to be entered by an approved cryptographic officer with compatible cryptographic key loader and software.

3.2.4 Modifying Cryptographic Processes

The Blackfin partitioning system and non-modifiable operating system provide the protections from operator and executing processes from modification of cryptographic processes. The software cannot be controlled from external sources except when a terminal device is connected to the DVP-200. These processes include:

- Reading Status information supplied by the module
- Loading Keys
- Zeroization of All Keys
- Operating mode changes

3.2.5 Separation of Cryptographic Boundaries

Separation of cryptographic boundaries will be handled by the virtual machine capabilities of the Blackfin microprocessor processor. The Blackfin partitioning system will only allow access to stored cryptographic software and data to authorized processes.

3.2.6 Audit Mechanisms

No audit mechanisms will be exercised in the DVP-200 Cryptographic Module. The application code, cryptographic data and critical security parameters are fixed entities in the Blackfin microprocessor and cannot be modified, accessed or deleted by process or operator intervention.

3.2.7 Cryptographic Keys and Critical Security Parameters

All Cryptographic Keys and CSPs are loaded (if applicable) and stored in plaintext.

The DVP-200 System Block Diagram is shown in Figure 5 Cryptographic Module Block Diagram. There are two main components that make up the DVP-200 System; the DVP-200 Cryptographic module and the Terminal Device.

The DVP-200 cryptographic module only generates keys used for key agreements public keys. The Key Generator PC generates the keys for the DVP-200 cryptographic module to store. It may act as the Key Fill device shown as a Key Loader and attaches to the DVP-200 cryptographic module. The DVP-200 cryptographic module's key management functions and controls for operations and receiving of the keys are contained within the Key Generator/Loader Application software.

The module generates cryptographic keys whose strengths are modified by available entropy. No assurance of the minimum strength of generated keys.

3.2.7.1 AES Keys

AES keys are loaded directly via a Terminal Device as depicted in Figure 5 Cryptographic Module Block Diagram or remotely via an OTAR process. (***NOTE:*** *The Terminal Device is not included in this evaluation*.) When functioning as a Key Loader, the Terminal Device shall be disconnected from all networks. Each key variable being loaded is accompanied with key index and a key check word that is calculated with a proprietary process as described in 3.2.7.1.3 Key Check Word . Upon receiving a key, the DVP calculates its own check word for the key and compares it against the received check word. If the check words match, the key is accepted and stored in both nonvolatile memory for future use and in volatile memory for immediate use. If the check words do not match, the key is rejected.

Once loaded, AES keys are inaccessible by any controls, commands, responses, and indicators.

AES keys may be zeroized via discrete input, Terminal Control Interface, or via the front panel.

For zeroizing via discrete input, refer to Table 13 – J1 Signal Names and Interfaces, pin 12,

Zeroizing via the Terminal Control Interface is performed when the DVP receives a "zero" command.

To zeroize keys via the front panel, press and hold the MODE button for five (5) seconds to enable scroll mode. When scroll mode is enabled, either keep the MODE button pressed until ZER is displayed or keep toggling the MODE button until ZER is displayed. When ZER is displayed, pressing the VALUE button for five (5) seconds will zeroize the AES keys.

3.2.7.1.1 Key Index

Each AES key is assigned an index, 1 – 8. Once the key has been loaded into the DVP, only the Key Index is selectable by the User. The Key Index is selectable via the front panel interface or Terminal Control.

3.2.7.1.2 Key Variable

The Key Variable is a 128-bit AES key represented by 32 ASCII characters, 0 – 9 and A – F.

3.2.7.1.3 Key Check Word

The Key Check Word is 32 bits in length represented by 8 ASCII characters, 0 – 9 and A – F. The Key Check Word is generated via a proprietary process in which the Key Variable is encrypted. A portion of the encryption output is used as the Key Check Word.

3.2.7.2 ECDH Keys

During the Public Key Exchange process, three ECDH keys are generated:

- Private Key
- Public Key
- Shared Secret

These items are stored in a volatile memory record. The entire Public Key is transmitted to the other DVPs. Upon completion of the exchange, the Shared Secret is generated.

During a normal PKE, a portion of the shared secret is used as an AES key. This AES key portion is stored in the volatile memory as an AES key. If the DVP is equipped with a front panel interface, three confirmation digits are momentarily displayed. The DVP operators may confirm with each other that they display the same digits. Other than the momentary display of the confirmation digits of the shared secret and the transmission of the Public Key, the ECDH keys generated are inaccessible by any controls, commands, responses, and indicators.

During a PKE used for authentication during the OTAR process, DVP transmits its Public Key. Other than the transmission of the Public Key, the ECDH keys generated are inaccessible by any controls, commands, responses, and indicators.

ECDH keys may be zeroized by cycling power on the DVP and by using the same processes described for zeroizing AES keys described 3.2.7.1 AES Keys.

3.2.7.3 PIN

The PIN is used during the OTAR authentication process and is treated as an AES key with the exception that it may be loaded with or without a check word. If it is loaded without a check word, the DVP generates a check word for it prior to storing it in nonvolatile memory.

Once loaded, as in the AES keys, the PIN is inaccessible by any controls, commands, responses, and indicators.

The PIN may be zeroized by using the same processes described for zeroizing AES keys described 3.2.7.1 AES Keys.

3.2.7.4 RNG Seed

The initial seed is a SHA-1 hash output based upon the DVP's programmed UID, PIN, and running time where running time is a meter of how long the DVP has been powered up in its lifetime. After the initial seed, each time the output of the RNG is used in a transmission or is used to generate an ECDH key, the last random number is stored in nonvolatile memory and is used as the seed the next time the DVP is powered up or reseeded. In addition to seeding the RNG at power up, the RNG is periodically reseeded during normal operation.

3.2.7.5 RNG Key

The initial RNG key is a fixed value within the DVP. Once the RNG has been seeded, all subsequent RNG keys is the SHA-1 hash output of the stored random number generated from the DVP and the running time(refer to 3.2.7.4 RNG Seed for more information on the running time). The RNG key only changes when power is cycled.

3.3 Module Maintenance

The cryptographic module does not support a field maintenance role. The only field maintenance is in the form of operator induced self tests.

The module's keys can be zeroized by the factory reset command via a control terminal, a zeroize command from the terminal device (Key Loader), through a discrete zeroize signal initiated by the operator, or though the DVP's front panel control.

The maintenance procedures are performed at a service depot or at a factory where the module can be resealed with the proper tamper evident tapes. Detailed procedures are beyond the scope of this document. The tamper evident tapes are supplemental protection covered in Section 3.6.1 Supplemental Module Protection.

3.4 Self Tests

3.4.1 Power On Self Tests

Power On Self Tests are described in Section 3.2.2.1.4.1 PBIT.

3.4.2 Conditional Tests

The DVP utilizes several conditional tests which are executed during self tests such as PBIT or during normal operational checks for CBIT activities. Table 10 – DVP-200 Conditional Tests

Table 10 – DVP-200 Conditional Tests

Test	Performed By	Condition	Description
AES GFS Box Test	Core A	PBIT, FBIT, IBIT	AES ECB mode "encrypt" KAT.
AES ECB Monte Carlo Test	Core A	PBIT, FBIT, IBIT	AES ECB Monte Carlo "encrypt" KAT.
AES OFB Test	Core A	PBIT, FBIT, IBIT	Fills a "start plaintext" buffer with random values and encrypts it using OFB mode filling a ciphertext buffer. The ciphertext buffer is then decrypted where the decrypted values are placed into "decrypted plaintext" buffer. The "start plaintext" buffer is compared to the "decrypted plaintext" buffer. The test passes if the values match.
CRNG Test	Core A	PBIT CBIT FBIT, IBIT	Verifies the new random number is not identical to the previous random number.
ECDH PK Test	Core A	PBIT, FBIT, IBIT	Simulated a key agreement between two entities. Verifies the two Shared Secrets generated from a simulated PKE match.

Test	Performed By	Condition	Description
Software Integrity Test	Core B	PBIT, FBIT, IBIT	The region in nonvolatile memory where the DVP firmware resides is read, a checksum of this region is computed and verified it is the expected value.
Nonvolatile data records	Core B	PBIT, FBIT	Performs tests to verify data in non-volatile memory is read correctly
Discrete line	Core B	PBIT, IBIT	Performs tests to verify the discrete lines inputs/outputs are functioning correctly.
FBIT Discrete Tests	Core B	FBIT	Performs tests to verify the discrete lines inputs/outputs are functioning correctly.
Internal timers	Core B	PBIT, FBIT, IBIT	Performs checks to verify the internal timers are functioning correctly.
PIC Processors	Core B	PBIT, FBIT, IBIT	Performs checks to verify the PIC processors are functioning properly.
Watchdog Test	Core B	FBIT	Verifies the hardware watchdog is functioning properly.
Tone Test	Core A	FBIT	Verifies the transmit and receive audio ports are functioning properly.
Data Buffer Test	Core B	PBIT, FBIT, IBIT, CBIT	Verifies the data buffers are cleared upon power up, entering self test modes, and mode changes. Mode changes include toggling between private (encrypted) mode and clear (unencrypted) modes.

3.5 Logical Interfaces

Logical interfaces include the front panel display and rear connector.

Table 11 – External Device Interfaces lists the logical interfaces for external devices.

Table 11 – External Device Interfaces

Logical Interface	Brief Description	Physical Port(s)	FIPS 140-2 Interfaces
Terminal Control Interface	ASCII control to configure and control the DVP including loading keys and OTAR.	Pins 17 - 19	Control Input Status Output Data Output
User Interface	Primary user interface to the DVP. These interfaces include PTT, transmit and receive audio, zeroize, tune in progress, and audio configuration.	Pins 1 – 13, 31 – 34	Control Input Data Input Data Output
User Data Terminal Interface	User data source and recipient.	Pins 14 - 16, 20 - 24, 39 - 46	Control Input Data Input Data Output
Radio Interface	Transmit and receive voice and data.	Pins 47 – 51, 53 - 55	Data Input Data Output

Note: All physical ports are located on J1 (refer to Table 13 – J1 Signal Names and Interfaces) unless stated otherwise.

3.5.1 Front Panel Display

The front panel is shown in Figure 2 - DVP 200 Standard Front Panel (822-2506-002 Rev B / Rev C) Cryptographic Module. The panel has a MODE button, VALUE button, and a LCD display. These items are described in Table 12 – Front Panel Display Interfaces.

Table 12 – Front Panel Display Interfaces

Logical Interface	Brief Description	Physical Port(s)	FIPS 140-2 Interfaces
MODE Button	Used to change operating modes	MODE Button	Control Input
VALUE Button	Used to activate zeroization, activate IBIT, and change settings such as AES key index, volume level, etc.	VALUE Button	Control Input
LCD Display	4-character display used to display the current mode, status, or setting.	LCD Display	Status Output

3.5.2 Rear Connector, J1

Figure 7 DVP-200 Rear Apron (Showing J1 Connector shows the rear view of the DVP). Figure 8 Connector J1 Pin Configuration illustrates J1 Rear Connector. Table 13 – J1 Signal Names and Interfaces lists P1's signal names interfaces.

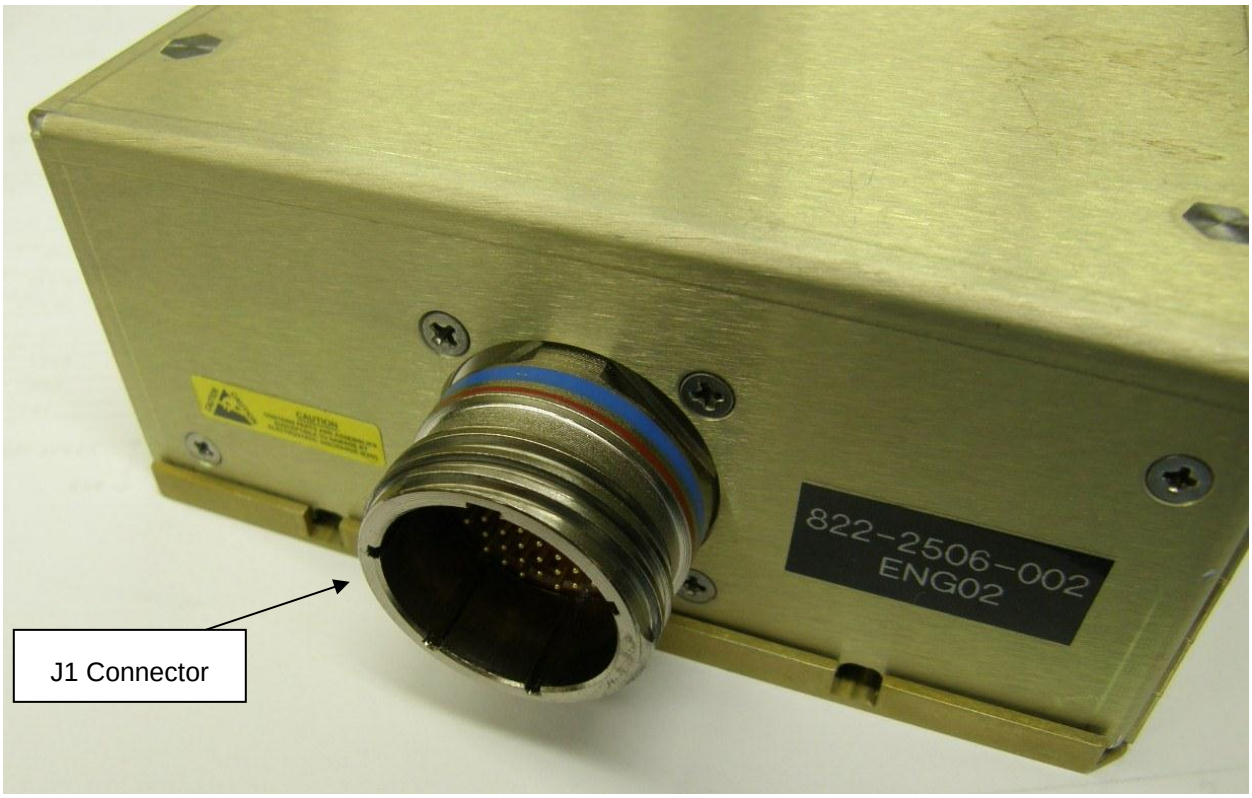

Figure 7 DVP-200 Rear Apron (Showing J1 Connector)

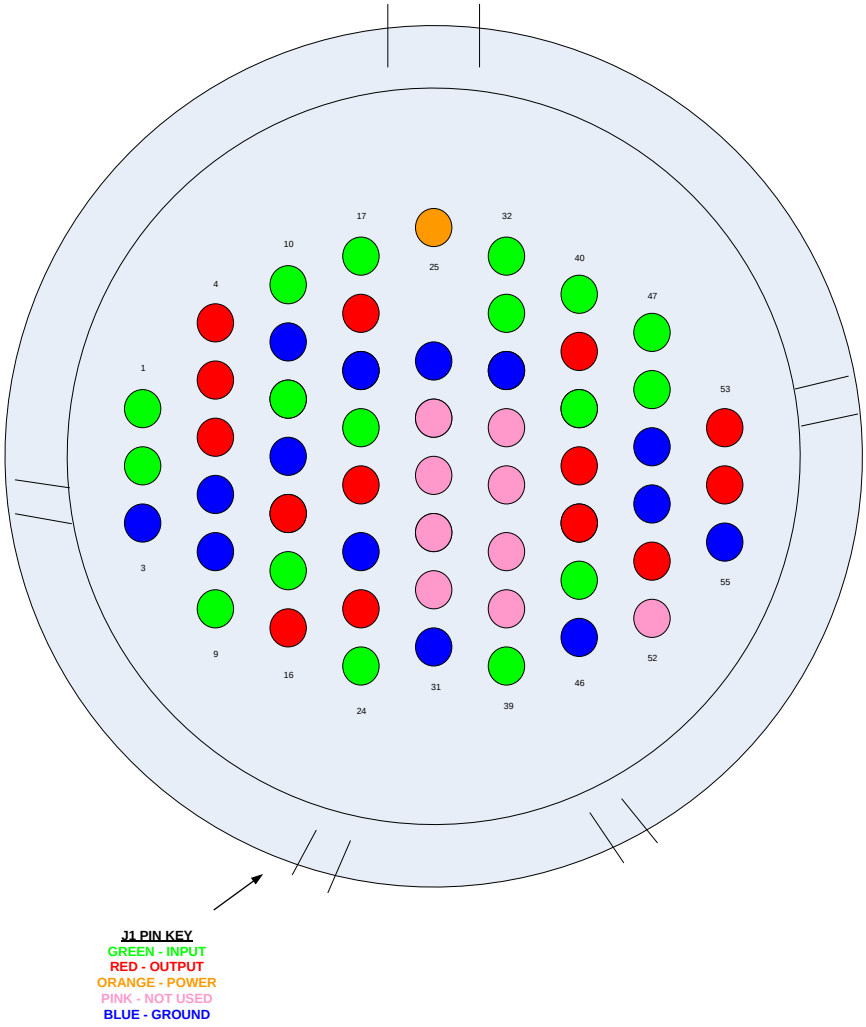

Figure 8 Connector J1 Pin Configuration

Table 13 – J1 Signal Names and Interfaces

Pin Number	Signal Name	Brief Description	FIPS 140-2 Interfaces
1	XMIT AUDIO IN	Transmit audio input	Data Input
2	XMIT AUDIO IN RTN	Transmit audio input return	Data Input
3	XMIT AUDIO IN SHIELD	Shield for transmit audio input	N/A
4	RCV AUDIO OUT 600 OHM	Receive audio output, 600 ohm	Data Output
5	RCV AUDIO OUT 150 OHM	Receive audio output, 150 ohm	Data Output
6	RCV AUDIO OUT RTN	Receive audio output return	Data Output
7	RCV AUDIO OUT SHIELD	Receive audio output shield	N/A
8	PUSH TO TALK GND	Ground for Push To Talk	N/A
9	PUSH TO TALK	Push To Talk discrete input. When enabled, the DVP will process audio received at XMT AUDIO IN, pin 1.	Control Input
10	PRIVATE SELECT	Private Select Discrete: When enabled only secure transmissions and reception of secure data is allowed	Control Input Status Output
11	PRIVATE SELECT GND	Ground for Private Select Discrete	N/A
12	ZEROIZE	Zeroize discrete input. When active, the DVP will be zeroized.	Control Input
13	ZEROIZE GND	Ground for zeroize discrete input	N/A
14	USER CTS	RS-232 Clear-To-Send (CTS) input/output line for the User port	Control Input, Status Output
15	USER IN CLK	RS-232 clock line for the User input port	Control Input Status Output
16	USER OUT CLK	RS-232 clock line for the User output port	Control Input Status Output
17	SERIAL CONT IN	ASCII serial control data input	Control Input, Data Input
18	SERIAL MON OUT	ASCII serial control data output	Status Output Data Output
19	SERIAL DATA RTN	ASCII serial control data return	Status Output Data Output
20	USER RXD	RS-232 receive data input line for the User port	Data Input
21	USER TXD	RS-232 transmit data output line for the User port	Data Output
22	USER RTN	RS-232 ground for the User data port	N/A

Pin Number	Signal Name	Brief Description	FIPS 140-2 Interfaces
23	USER DCD	RS-232 Data Carrier Detect (DCD) input/output line for the User port	Control Input Status Output
24	USER RTS	RS-232 Ready-To-Send (RTS) input/output line for the User port	Control Input Status Output
25	POWER	DVP power	N/A
26	POWER GND	Ground for DVP power	N/A
27	N/C		N/A
28	N/C		N/A
29	N/C		N/A
30	N/C		N/A
31	TUNE IN PROGRESS GND	Ground for Tune In Progress	N/A
32	TUNE IN PROGRESS	Tune In Progress discrete input.	Control Input
33	AUDIO CONFIGURATION	Audio configuration input discrete. When enabled, the audio gain is increased by 10 decibels (dB)	Control Input
34	AUDIO CONFIGURATION GND	Ground for the audio configuration discrete	N/A
35	N/C		N/A
36	N/C		N/A
37	N/C		N/A
38	N/C		N/A
39	RADIO CTS	RS-232 CTS input/output line for the Radio port	Control Input Status Output
40	RADIO RXD	RS-232 receive data input line for the Radio port	Data Input
41	RADIO TXD	RS-232 transmit data output line for the Radio port	Data Output
42	RADIO IN CLK	RS-232 clock line for the Radio in port	Control Input Status Output
43	RADIO OUT CLK	RS-232 clock line for the Radio output port	Control Input Status Output
44	RADIO RTS	RS-232 RTS input/output line for the Radio port	Control Input Status Output
45	RADIO DCD	RS-232 DCD input/output line for the Radio port	Control Input Status Output
46	RADIO DATA RTN	Radio data return	N/A
47	RCV AUDIO IN	Receive audio input	Data Input
48	RCV AUDIO IN RTN	Return for the receive audio input	Data Input
49	RADIO DATA RETURN	Return for the receive data input	Data Input

Pin Number	Signal Name	Brief Description	FIPS 140-2 Interfaces
50	KEYLINE OUTPUT GND	Ground for the keyline output	N/A
51	KEYLINE OUTPUT	Keyline output discrete	Status Output
52	N/C		N/A
53	XMIT AUDIO OUT	Transmit audio output	Data Output
54	XMT AUDIO OUT RTN	Transmit audio output return	Data Output
55	XMT AUDIO OUT SHIELD	Shield for transmit audio output	N/A

3.6 Mitigation of Other Attacks Policy

DVP-200 is subject to a range of generic threats applicable to most cryptographic modules processing sensitive information. Potential threats exist to the confidentiality and integrity of the information processed, stored, and transmitted by the module. Natural disasters and damage can result from fire, water, wind, and electrical sources. Man-made threats are from those who would target the DVP-200 for espionage, criminal activity, unlawful use, denial of service, or malicious harm. External and internal threats include espionage services, terrorists, hackers, and vandals.

System break-in statistics indicate the greatest threat(s) to DVP-200 are likely to come from an insider. The most likely scenario involves an authorized user who accidentally or inadvertently commits or omits some action that damages or compromises the module, one of its components, or information processed, stored, or transmitted by the module. The next most likely scenario involves an authorized user who takes deliberate action to damage the module, one of its components, or its data for personal gain or vengeful reasons. Such a person could also engage in espionage, other criminal activity, or exploitation of system assets for personal gain. There is the threat of co-option of: users with authorized access to the module, support personnel, or facilities employees with physical access to the module components arising from motivation for financial gain. There is also the threat posed by disgruntled employees, especially those who are to be terminated for cause.

In addition, there is a threat posed by module users who negligently or inadvertently fail to follow security requirements. Finally, there is the threat arising from the failure of authorized users to employ proper procedures for the entry or manipulation of module data, this is often due to the failure to train personnel in the proper use and operation of the module.

Other threats include natural disasters and system failures, accidents and errors, and hostile acts by humans. Threat agents can include storms, sand storms, earthquakes, floods, and extremes of hot and cold temperatures. They also include software design errors and operator errors. In addition, hostile users, thieves, terrorists, and saboteurs, can all be brought to bear against the system. Combat forces together with their weapons and electronic warfare capabilities are significant threats to the system. Threats and threat agents are resisted by the system itself (e.g., the security features in the hardware and software) and by the security practices and standard operating procedures that constitute the total operating environment within which the system operates. In the DVP-200 risk assessment model depicted in Figure 9 DVP-200 Risk Assessment Model, threats and threat agents may attack the system while performing in the total operating environment. Other mitigations to attacks beyond FIPS Security Level 1 are described in 3.6.1 Supplemental Module Protection.

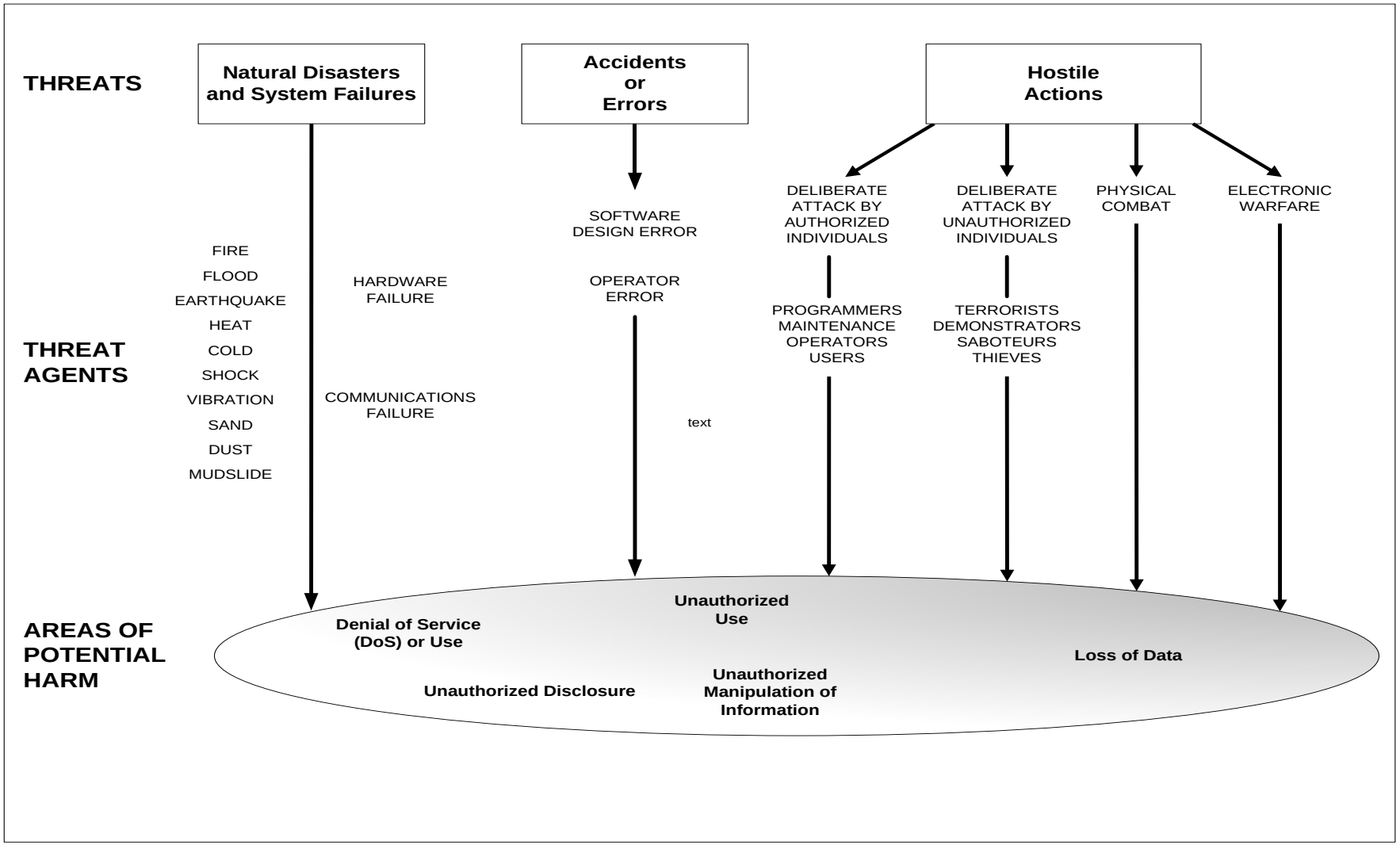

Figure 9 DVP-200 Risk Assessment Model

3.6.1 Supplemental Module Protection

The following are additional supplemental protection for the module. The physical security mechanisms in this section are addressed in FIPS 140-2 Level 2 but have not been tested for modules in this security policy. There is no assurance of physical protection or correct operation of the DVP-200 supplemental security mechanisms.

The DVP-200 employs supplemental physical security via the use of:

- Tamper evident tape
- Weep holes
- flanges
- blind screw holes
- tamper-evident coating
- tamper-proof filler

These methods are used to deter direct observation, probing, or manipulation of module components and to provide evidence of attempts to tamper with or remove module components.

3.6.1.1 Tamper-Evident Tape

Mounting hardware that is exposed to the outside of the DVP-200 enclosure is covered with tamper-evident tape. These items/areas include select screw heads such that the DVP cannot be opened without damaging the tamper evident tape. Figure 10, Figure 11, and Figure 12 illustrate the locations of the tamper evident tape.

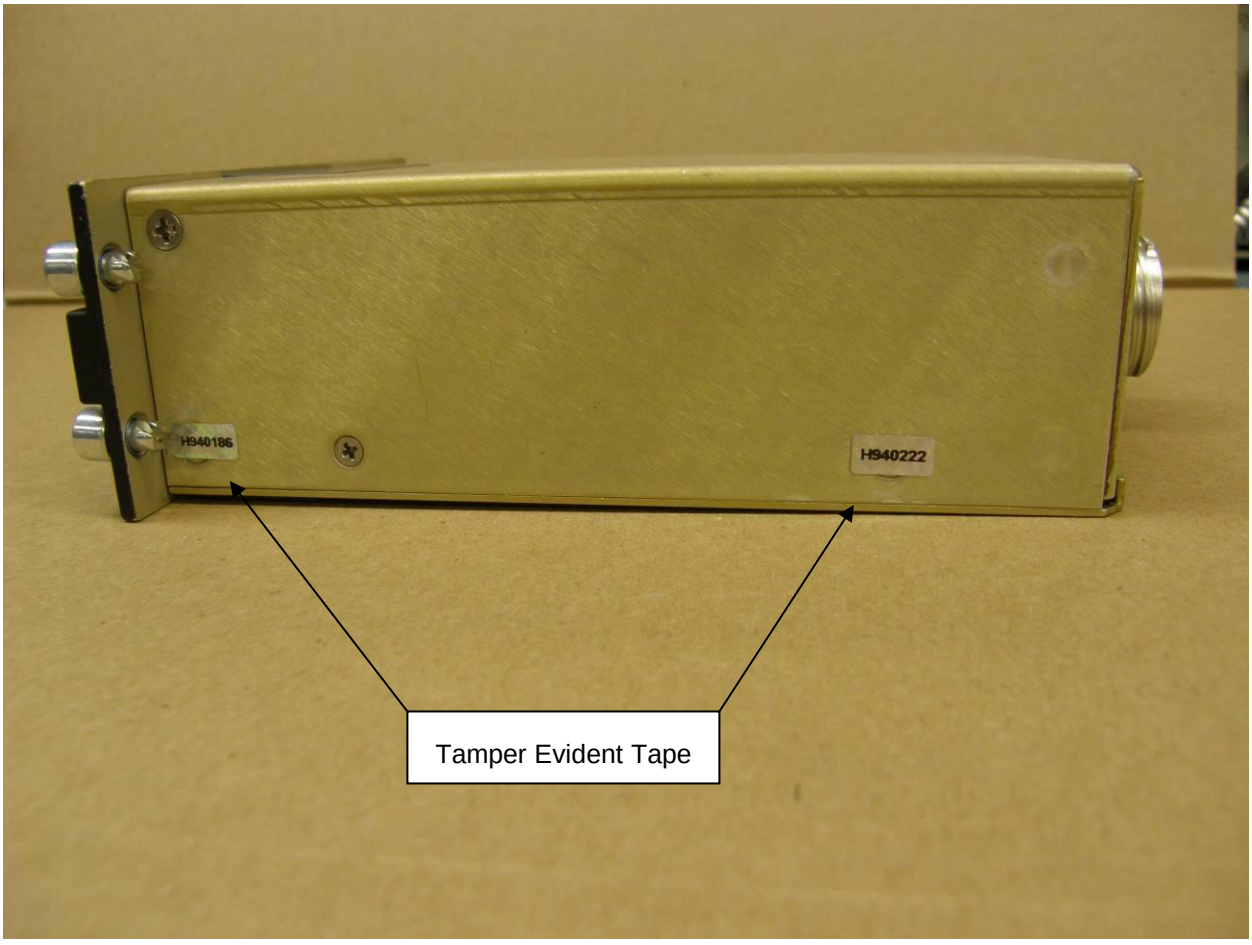

Figure 10 DVP-200 Tamper Evident Tape Right Side

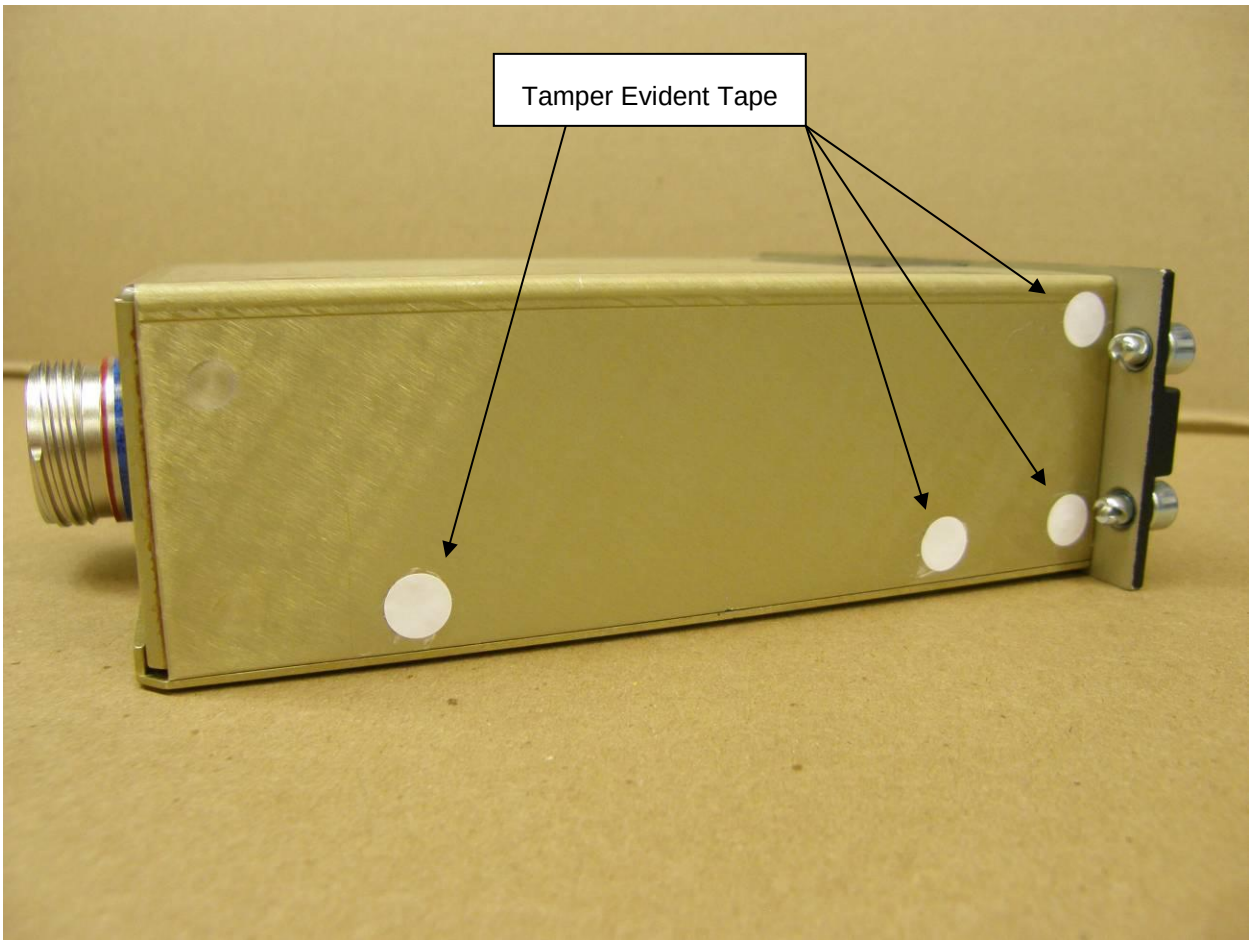

Figure 11 DVP-200 Tamper Evident Tape Left Side

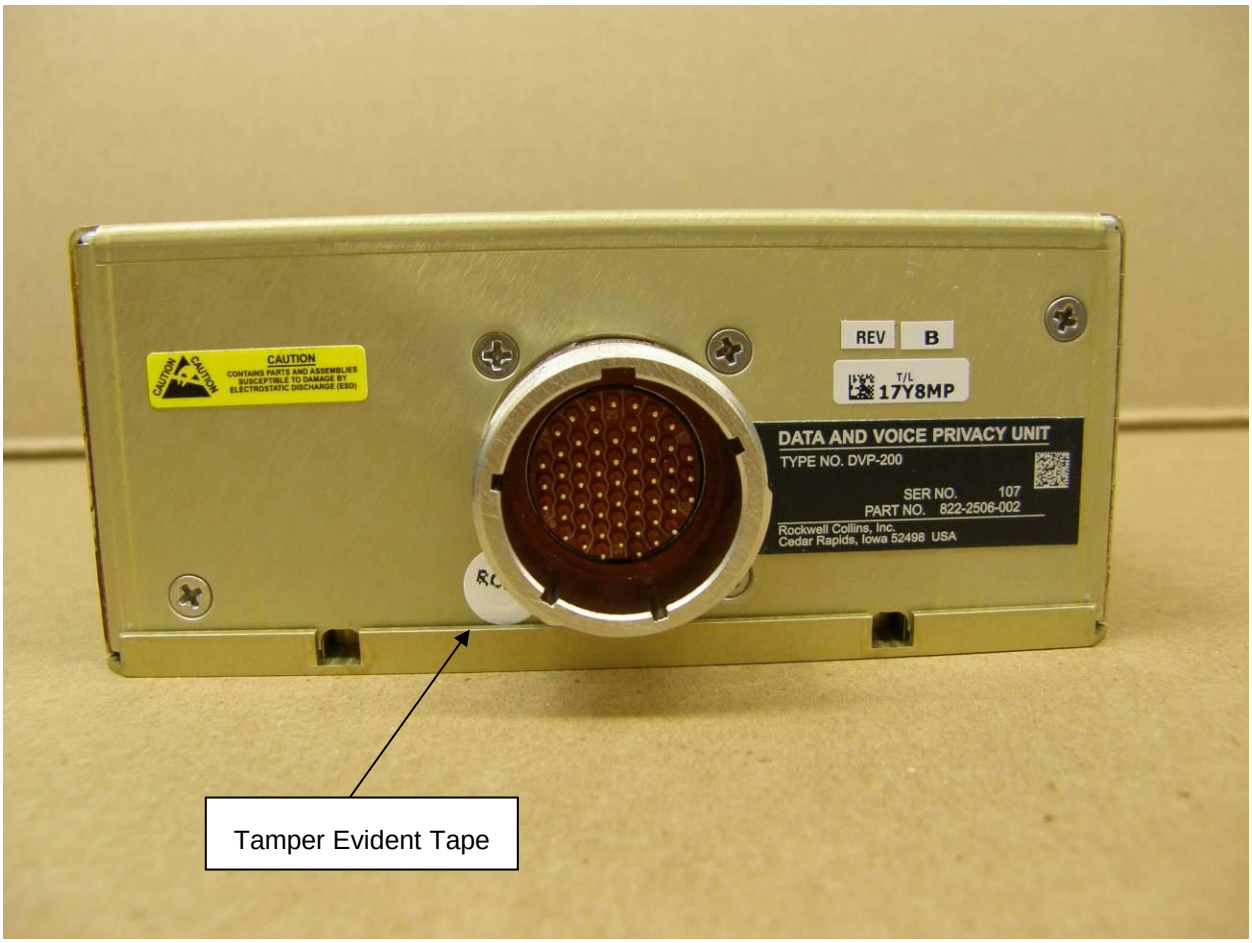

Figure 12 DVP-200 Tamper Evident Tape Rear

3.6.1.2 Weep Holes

The DVP-200 has two weep holes located on the bottom edge of the rear apron. These holes allow condensation to escape from the enclosure. The holes are internally blocked to preclude the insertion of a flexible fiber optic probe.

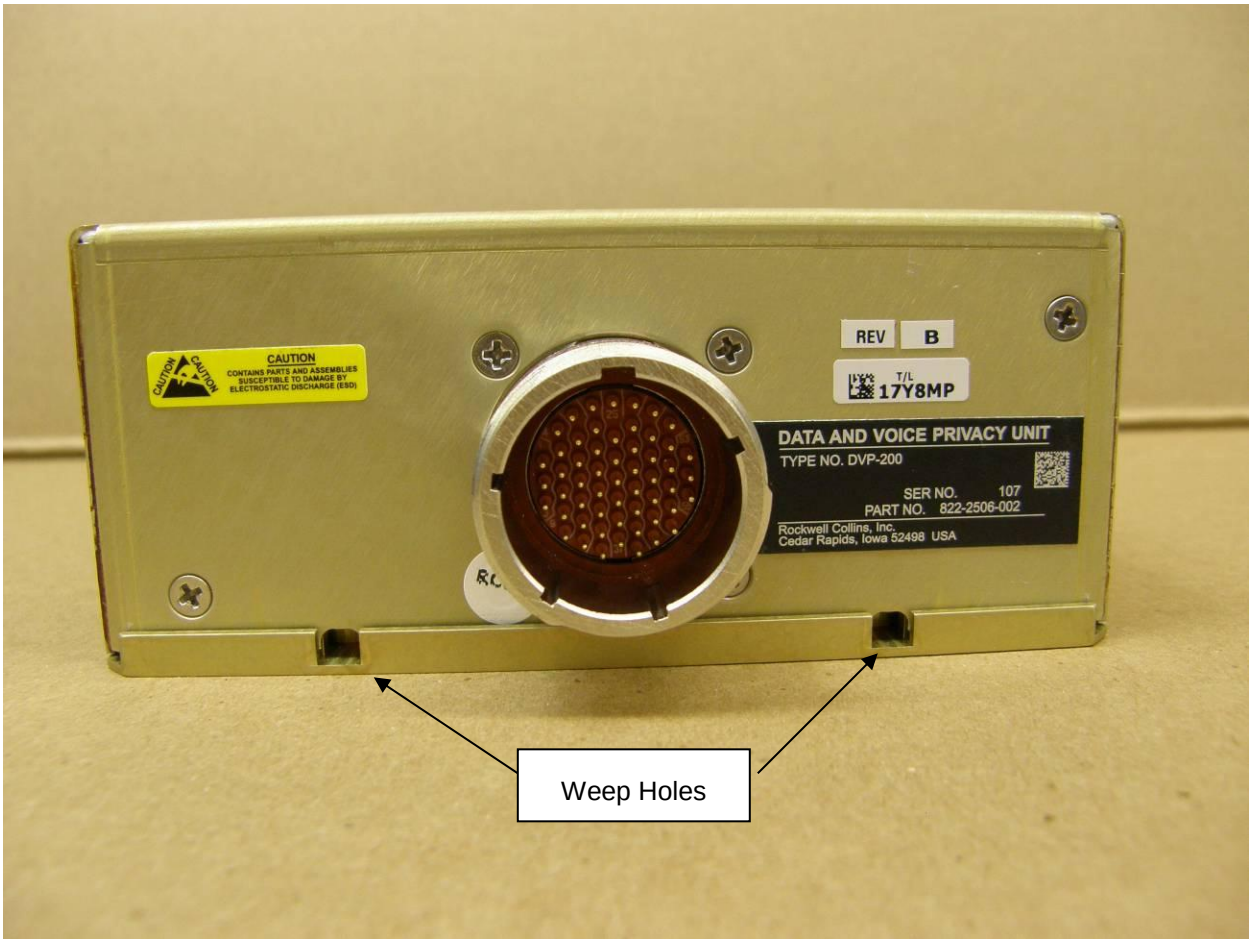

Figure 13 DVP-200 Weep Holes

3.6.1.3 Flanges and Blind Screw Holes

The bottom cover has flanges to allow for weep hole ventilation yet provides barriers against the insertion of a flexible fiber optic probe. Also the two rear corners have flanges to provide similar protection. The side flanges contains mounts for screws in which the screw mounts are blind such that if a screw is removed a probe cannot be inserted. Figure 14 illustrates these features.

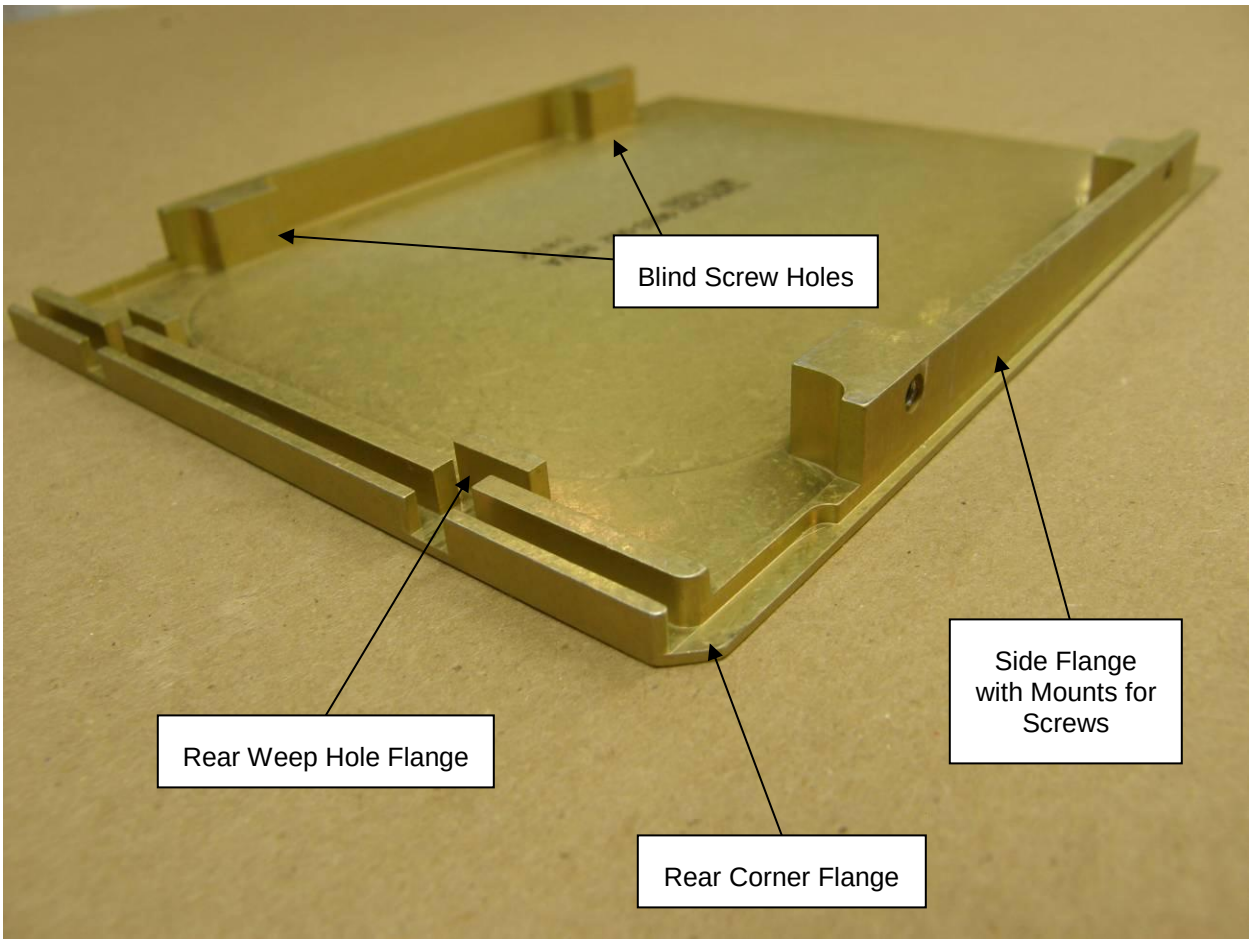

Figure 14 DVP-200 Bottom Cover

3.6.1.4 Tamper-Proof Filler and Tamper-Evident Coating

The DVP's enclosure openings are filled with a tamper-proof filler or potting material to deter direct observation, probing, or manipulation of module components. The tamper-evident coating is opaque within the visible spectrum. This material is applied to the opening from the inside of the enclosure, covering all holes that are part of the manufacturing process. These holes include relief holes in the enclosure's corners that allow bending of the sheet metal. The filler is shown in Figure 15.

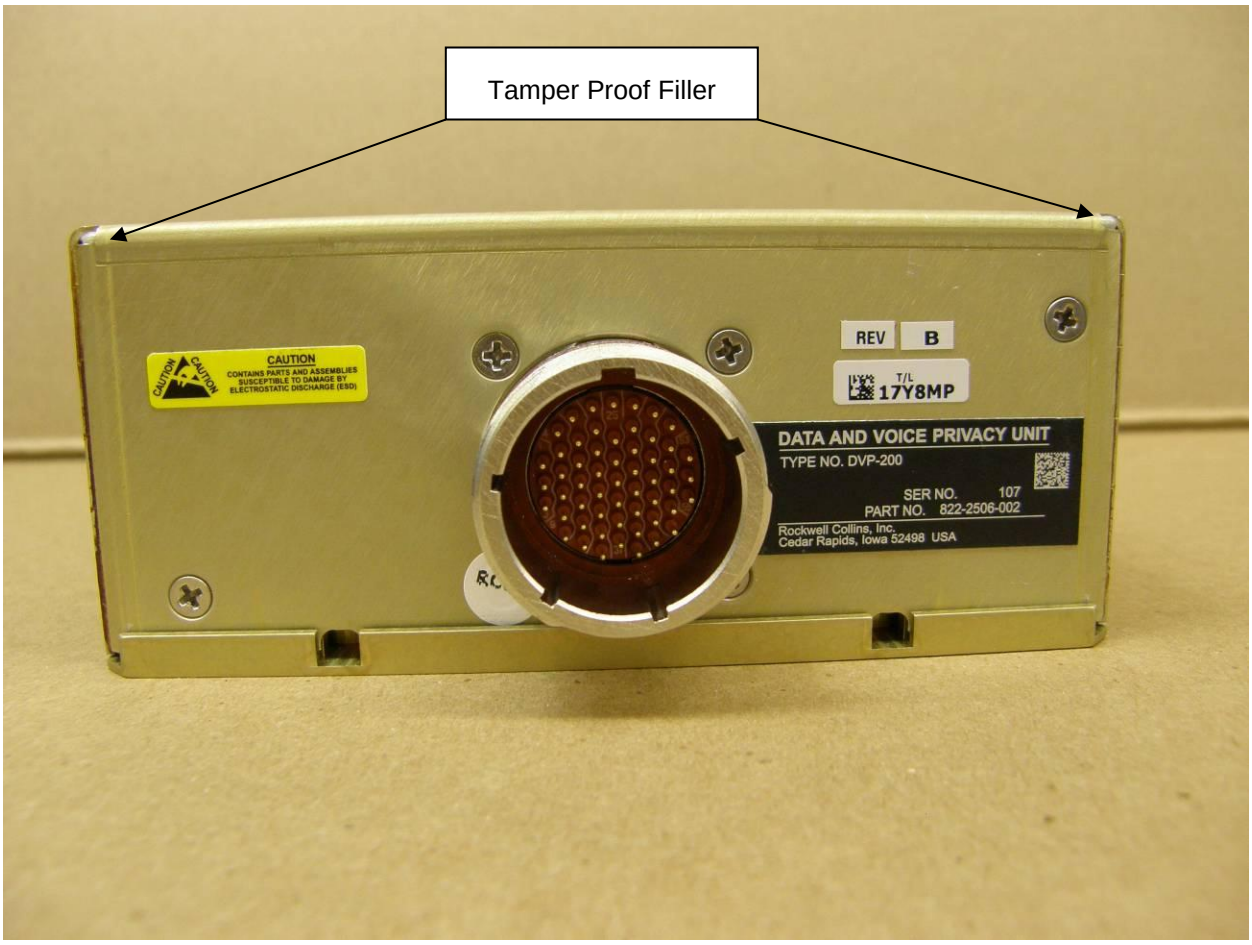

Figure 15 DVP-200 Tamper Proof Filler

3.6.2 Circuit Card Assembly Coating

The EMI/Power board and the Main Processor board are conformal coated for added physical protection against moisture.

3.6.3 FIPS Approved Module Confirmation

Upon receiving the unit, the User (the User may be a Crypto Officer) should inspect the following for evidence of tampering:

- Tamper evident tape is intact and does not show signs of tampering (refer to Section 3.6.1.1 Tamper-Evident Tape).
- All corners remain sealed with the tamper proof filler (refer to Section 3.6.1.4 Tamper-Proof Filler and Tamper-Evident Coating.
- The unit as a whole does indicate the inside of the DVP was accessed.

Once the unit has been inspected, the unit should be powered up and verified it passes PBIT. If there is no evidence of tampering and the unit passes PBIT, the unit is confirmed to be a FIPS Approved Module.

If the unit is not confirmed to be a FIPS Approved Module, the User should report the findings to the appropriate personnel.

4 Acronyms and Abbreviations

The purpose of this section is to list of terms acronyms that are used in this document.

AES	Advanced Encryption Standard
BIT	Built-In Test
CODEC	Coder/Decoder
CMVP	Cryptographic Module Validation Program
CSP	Critical Security Parameter
DVP-200	Data & Voice Privacy Encryption Unit - 200
ECB	Electronic Code Book
EMI	Electro-Magnetic Interference
FIPS	Federal Information Processing Standard
HF-SSB	High Frequency-Single Sideband
MAC	Message Authentication Code
MB	Megabyte
MELPe	Mixed Excitation Linear Predictive enhanced
NATO	North Atlantic Treaty Organization
NIST	National Institute of Standards and Technology
OFB	Output Feedback
OTAR	Over-The-Air Rekey
RC	Rockwell Collins
RCPN	Rockwell Collins Part Number
RXD	Received Data
SDRAM	Synchronous Dynamic Random Access Memory
SPI	Serial Peripheral Interface
TXD	Transmit Data
UART	Universal Asynchronous Receiver/Transmitter

UHF	Ultra High Frequency
VHF	Very High Frequency