UNITED STATES MARINE CORPS
COMMAND ELEMENT
II MARINE EXPEDITIONARY FORCE
FLEET MARINE FORCE
PSC BOX 20080
CAMP LEJEUNE, NC 28542-0080

IN REPLY REFER TO
5500
G-6

JAN 21 2021

II MARINE EXPEDITIONARY FORCE POLICY LETTER 1-21

From: Commanding General, II Marine Expeditionary Force, FMF
To: Distribution List

Subj: II MEF TRANSMISSIONS SECURITY POLICY

Ref: (a) MFCC OPORD 20-011

Encl: (1) Enhanced Bandwidth Efficient Modem (EBEM) Guide
(2) Linkway S2 Modem Guide

1. Situation. Unprotected Commercial Satellite Communication (COMSATCOM) transmissions links are susceptible to cyberspace interference and exploitation.

2. Mission. Effective immediately, this Policy Letter directs all II Marine Expeditionary Force (MEF) Commands to enable Transmissions Security (TRANSEC) in order to secure COMSATCOM links.

3. Execution

a. Commander's Intent. Communications architectures supported by COMSATCOM links are protected from known vulnerabilities.

b. Concept of Operations. Conduct deliberate planning and implement technical control measures within II MEF to ensure high level of security to prevent detection, collection, radio fingerprinting, and traffic analysis of COMSATCOM architectures.

c. Tasks

(1) Commanding Generals, 2d Marine Division, 2d Marine Aircraft Wing, 2d Marine Logistics Group

(a) Enforce U.S. Marine Corps Forces Command (MARFORCOM), Headquarters Marine Corps (HQMC), Combatant Commands (CCMD), Defense Information Systems Agency (DISA), and Department of Defense (DoD) policies to enable TRANSEC on all COMSATCOM links.

(b) Comply with the directed actions in the coordinating instructions.

(2) Commanding Officers, II Marine Information Group, 22nd, 24th, and 26th Marine Expeditionary Units

(a) Enforce MARFORCOM, HQMC, CCMD, DISA, and DoD policies to enable TRANSEC on all COMSATCOM links.

(b) Comply with the directed actions in the coordinating instructions.

(3) II MEF AC/S G-6

(a) Enforce MARFORCOM, HQMC, CCMD, DISA, and DoD policies to enable TRANSEC on all II MEF COMSATCOM links.

(b) Publish enclosures on II MEF G-6 SharePoint for reference.

d. Coordinating Instructions. In accordance with reference (a), execute the following actions:

(1) Implement network segmentation on routers throughout networks to and from critical servers.

(2) Implement and enable TRANSEC on all Frequency Division Multiple Access (FDMA) COMSATCOM links to include both gateway and internal command links per enclosures.

(3) Implement and enable TRANSEC on all Time Division Multiple Access (TDMA) COMSATCOM links to include both gateway and internal command links per enclosures.

(4) Implement and enable TRANSEC on all Network Centric Waveform (NCW) Networking-on-the-Move (NOTM) COMSATCOM links to include both gateway and internal command links per enclosures.

(5) Implement separate operational and management traffic networks for COMSATCOM links.

(6) Ensure all modems are HQMC Command, Control, Communications, and Computers (C4) approved and compliant with Security Technical Implementation Guides (STIG).

(7) Ensure all modems have different and unique passwords that are only released to personnel who have a need to know. Wherever technically feasible, the password requirement shall be 16 characters in length, with variation among numbers, upper/lower case letters, and special characters. Passwords must be changed quarterly (Jan, Apr, Jul, and Oct). Hard or digital copy lists of passwords must be stored in security containers controlled with SF 702 checklists.

(8) Ensure boot and option file transfers are secured. Although these files are all unclassified, they must be considered "Controlled Unclassified Information" (CUI) and treated accordingly. These files must only be sent to DoD Emails which are encrypted and digitally signed. When burning these files to disk, Marines must ensure physical control of the disks and/or store in security containers controlled with SF 702 checklists. Disks must be appropriately disposed of when no longer needed.

(9) Enclosure 1 contains instructions for implementing TRANSEC on the ViaSat EBEM.

(10) Enclosure 2 contains instructions for implementing TRANSEC on the ViaSat Linkway S2 modem.

(11) Units must coordinate with the gateway/teleport for TRANSEC requirements on all gateway/teleport missions.

(12) Gateway and Worldwide Reachback (WWRB) will provide satellite operators with TRANSEC procedures for all iDirect modem missions.

4. Administration and Logistics. The point of contact for this matter is the II MEF G-6 Operations Officer at (910) 451-7274 or the Assistant Operations Officer at (910) 451-8956.

5. Command and Signal

a. Command. This Policy is applicable to the Marine Corps Total Force.

b. Signal. This Policy is effective the date signed.

B. D. BEAUDREAULT

Distribution: A/B

8. Press the down arrow key and follow the prompts to input a new ADMIN and USER password.

9. After changing the passwords press the right arrow key two (2) times to get to **NEW RNG SEED**.

10. Press the down arrow key one (1) time and follow the prompts to enter a new RNG SEED via the keypad.

11. After the RNG SEED is accepted press the right arrow key one (1) time to get to **NEW SMA TOKEN**.

12. Press the down arrow key one (1) time and follow the prompts to enter the new SMA TOKEN via the keypad.

13. After the SMA TOKEN is accepted press the up arrow key until you get back to **ENCRYTION CHANGE PARAMS**.

14. Pres the left arrow key one (1) time to get to **ENCRYPTION CONTROL**.

15. Press the down arrow key one (1) time to get to **ENCRYP ENABLE.**

16. Press the enter key, an asterisk (*) should appear next to OFF.

17. Press the right arrow key one (1) time to change the option to ON.

18. Press enter to accept the change.

19. When UNIT WILL REBOOT = YES, press enter to accept.

20. EBEM will reboot.

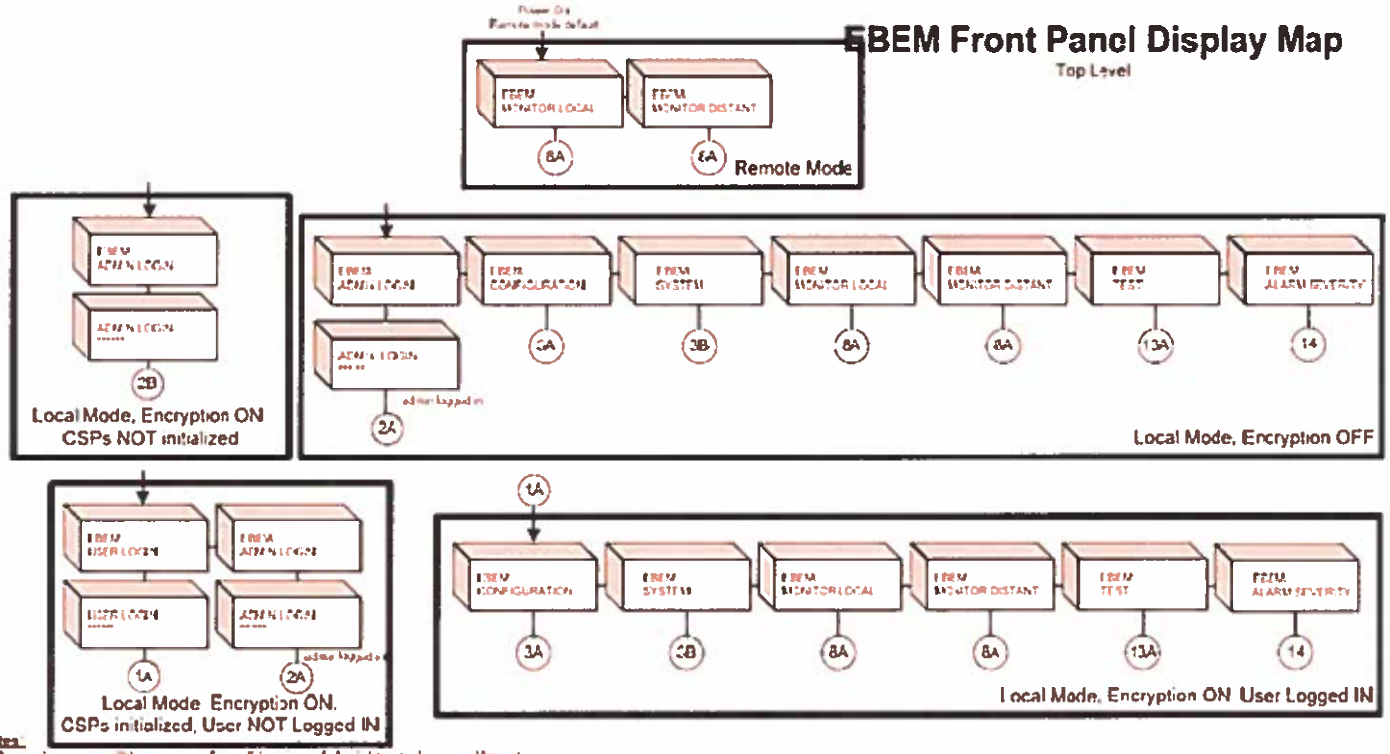
21. Once the EBEM is completely rebooted the ENCRYPTION ACTIVE LED should be GREEN. The BYPASS LED will be off. The ACTIVE KED will blink T (dash) or R (dot dash dot) in Morse code when the transmit or receive encryption is out of lock.

22. Once this is complete the modem is ready for operational configuration per the mission SAA.

Reference included diagrams for the EBEM menu tree maps.

EBEM Front Panel Display Map

Top Level



Notes:

1. On each screen will be prompts for valid actions: left, right, up, down and/or enter.
2. For fields which may be changed, pressing the enter key enters edit mode - a flashing cursor appears. If the value of the field is selected from a list, use the left and right arrow keys to move between choices. If the value is entered via the keyboard, use the left and right arrow keys to select the character position, then enter the appropriate character. Press Enter key to accept the edited value, or press up to cancel, leaving the value unchanged.
3. Entry of alphabetic characters is context sensitive. For entry of characters in an alphabetic field, pressing a given key 1, 2 or 3 times in quick succession causes entry of the first, second or third alphabetic character.
4. When in edit mode, the last entered value is flagged with *.
5. List items are shown in their entirety. During configuration, some lists items will not be displayed, based upon previously entered configuration data. For example, when Encryption is ON, CONFIGURATION EDIT - TX_MODE list contains only EBEM and CW. When Encryption is OFF, CONFIGURATION EDIT - TX_MODE list contains MIL-188A, IESS-308, IESS-309, IESS-310, EBEM and CW.
6. ZEROIZE PROCEDURE: Pressing and holding the *, - and 0 shaded keys simultaneously will return the unit to the factory default state. Follow instructions on front panel display.

Enclosure (1)

JAN 21 2021

JAN 2 1 2021

EBEM Front Panel Display Map

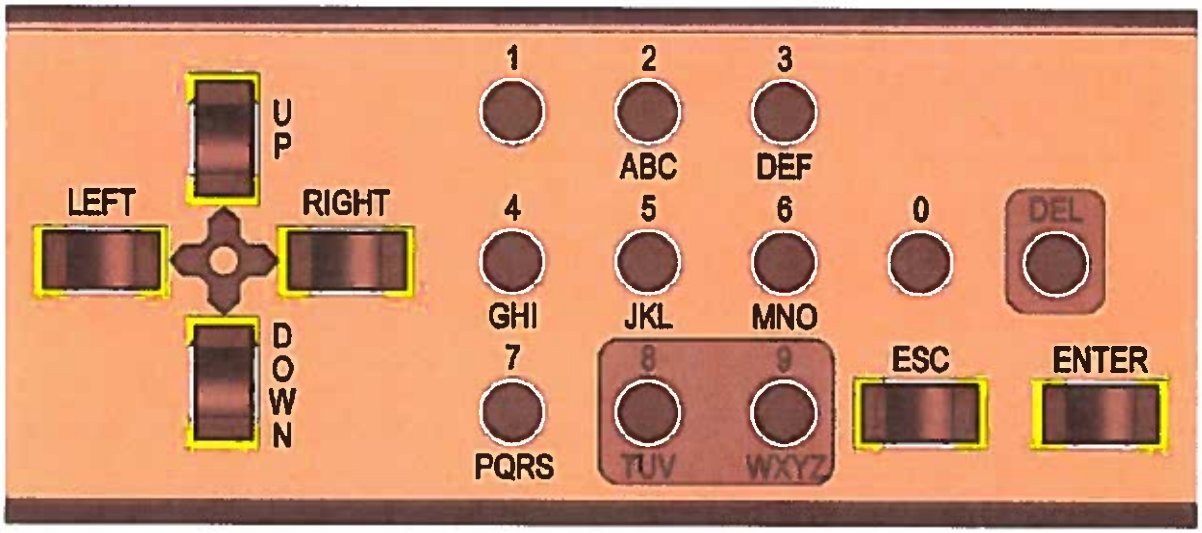
Encryption Configuration

Enclosure (1)

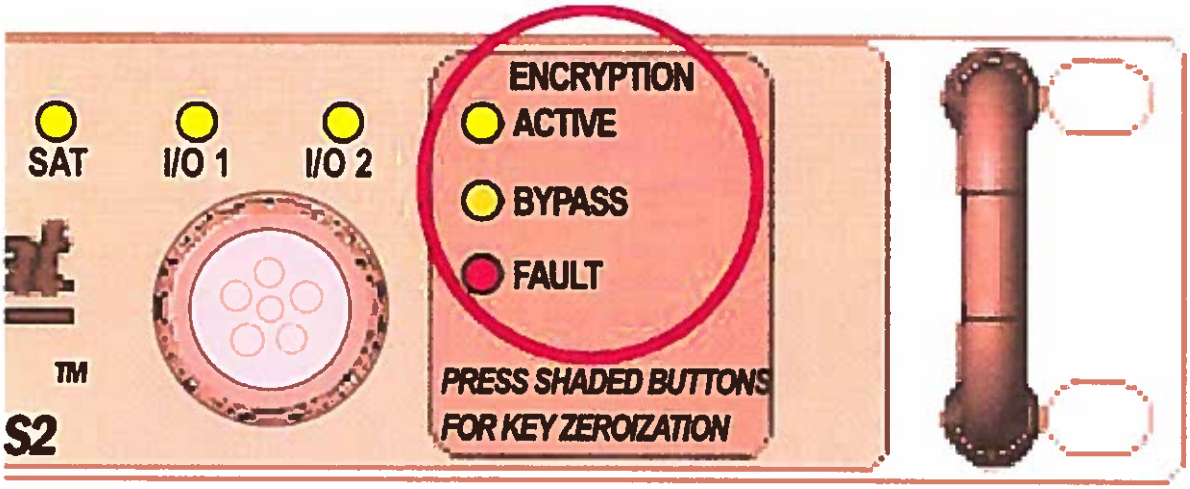
This guide explains how to place a Linkway S2 modem into zero, bypass, or load TRANSEC.

Zeroization:

How to manually zeroize the modem from the front panel.
Using the front panel keypad (Figure), simultaneously press and hold the three shaded keys (8, 9, and DEL).



The local modem operator verifies modem is fully zeroized by confirming the ACTIVE and FAULT Encryption LEDs are flashing (Figure). Solidly lit LEDs do not indicate a zeroized modem.



The following steps configure a new or zeroized LinkWays2 modem for encryption using the modem's front panel controls and LCD. Note that a new or zeroized LinkWay S2 modem will have no traffic keys, the Active LED will be flashing green, and the Fault LED will be flashing red.

1. Press **Enter** to display the top level menu items.
2. Press the **RIGHT** or **LEFT arrow** to scroll to the Admin Login menu item and then press **Enter**.
3. Enter the default Admin password: *123456789* and then press **Enter**.
4. Enter and verify the new 8 digit minimum Admin password.
5. Press the **RIGHT** or **LEFT arrow** to scroll to the User Password menu item and then press **Enter**.
6. Enter and verify the new 8 digit minimum User password and then press **Enter**.
7. Press the **RIGHT** or **LEFT arrow** to scroll to the Encryption Mode menu item and then press **Enter**.
8. Press **1** for encryption enabled; press **2** for encryption bypassed.
9. If the configuration was changed, verify the new configuration by pressing **9**.
10. If the configuration was changed, power-cycle the modem.

If encryption is enabled, valid keys must be loaded into the LinkWays2 modem by using the simple key loader (SKL). Follow the steps below to perform SKL key loading.

1. Power on the LinkWays2 modem.
2. Press **Enter** to display the top level menu items.
3. Press the **RIGHT** or **LEFT arrow** to scroll to the Admin Login menu item.
4. Press **Enter** and then enter the Admin Password.
5. Power on the SKL, and double click the "**Corelib**" icon.
6. Enter the username and password.
7. When the startup information screen appears, click **Okay**.
8. Select the **Keys** tab.
9. Select the desired key from the displayed list.
10. Click the "**Send**" icon at the top of the screen.
11. Verify the settings and then click **Okay**.
12. When the "**Ready to send**" screen is shown, connect the SKL to the audio connector on the front of the modem and then click **Okay** on the SKL.
13. Wait for the verification message on the SKL then click **Okay**.
14. Verify that the key was loaded by viewing the LCD on the modem's front panel.
15. Press **Enter** on the front panel to assign the key.
16. Press **1** to assign the key as the Primary key.
17. Logout as Admin or power-cycle the terminal.

V3k-100 equipped Linkway modem LED matrix.

SECURITY CARD STATE*	ACTIVE LED	BYPASS LED	FAULT LED
Booting	OFF	OFF	ON
Fully Zeroized	Flashing	OFF	Flashing
Bypassed and Partially Zeroized	Flashing	ON	OFF
Bypassed and Not Zeroized	OFF	ON	OFF
Active and Partially Zeroized	Flashing	OFF	OFF
Active and Not Zeroized and Not Ready	OFF	OFF	OFF
Active and Not Zeroized and Ready	ON	OFF	OFF
Security Card Fault	N/A	N/A	ON