Region 9 Army MARS Training Topics for "on-the-air" use

TRAINING TOPIC – AuthTables

LESSON INTENT – To Provide a Review the use of Auth Tables

REFERENCES – AM 6 Annex H Authentication Tables 18-M

EXPECTED TIME TO DELIVER – 50 Minutes

CONTENT OUTLINE & KEY POINTS –

1. PROCESS
2. STANDARDS
3. FAILURE TO AUTHENTICATE

MANUAL PROCESS – Using Auth Tables in AM 6 Annex H

The station beginning the authentication process will "challenge" the other station by selecting from the tables in this document:

- A table letter or the appropriate table for the time period.
    Note: When multiple tables are in use, the table letter representing a specific Table is selected. When tables are assigned by date/time period the table assigned to the date/time period is selected and no Table Letter is selected.

- Select two random letters from the table, consisting of
    a. A random letter (except Z) from LINE INDICATOR COLUMN of the selected table selecting a Line
    b. a random letter from the selected Line

The station will make a radio call in accordance with ACP-125 (G) section 619.

EXAMPLE – "**ALPHA ALPHA ALPHA THIS IS BRAVO BRAVO BRAVO, AUTHENTICATE BRAVO UNIFORM, OVER**"

3. The challenged station will "reply" with the cipher letter directly *below* the second letter in the challenge.

EXAMPLE – "**THIS IS ALPHA ALPHA ALPHA, I AUTHENTICATE INDIA, OVER**"

If the station that began the authentication process has not already been authenticated, the second station will then challenge the first station using the same procedure with a different random letter combination from the same table.

AUTOMATED PROCESS USING STATION MASTER

STANDARDS

To achieve this standard printed copies of the Authentication Tables should be readily available when operating.

• Within 15 seconds (not counting time taken by the other radio station), transmit using proper radio procedure, a two letter challenge, and from the reply, determine whether or not the station responded correctly.
• Within 15 seconds, using the correct radio procedure, respond to a challenge with correct authentication. If immediately challenged again, respond correctly within 5 seconds.

FAILURE TO AUTHENTICATE

Another challenge should be made if an incorrect reply is received, if a "standby" is requested, or if an unusual delay occurs between challenge and reply.

Failing to properly reply to a challenge three times shall be considered a failure to authenticate. Stations who fail to authenticate shall not be authorized net entry or the listing of traffic.
During **training** use, a failure to properly authenticate may be handled by telephone or e-mail to quickly get the offending station back into the net.

A station that is unable to authenticate with this publication, but that can communicate with MARS stations using an appropriate on-line or off-line encryption systems shall be considered properly authenticated.