Region 9 Army MARS Training Topics for "phone bridge" use

TRAINING TOPIC – Operations Security (OPSEC)

LESSON INTENT – The intent of this lesson is to discuss the measures MARS operators must take to preclude military information from falling into unfriendly hands. Practical exercises are included to generate discussion.

REFERENCE – OPLAN AM-3 Annex B

EXPECTED TIME TO DELIVER – 45 Min.

CONTENT OUTLINE & KEY POINTS

Operations Security (OPSEC) - We must always assume that our communications are being monitored, including radio network, telephone, faxes, e-mail and information posted to MARS web sites.

The Army defines OPSEC as "All measures taken to maintain security and achieve tactical surprise. It includes counter surveillance, physical security, signal security, and information security. It also involves the identification and elimination or control of indicators that can be exploited by hostile intelligence organizations."

- OPSEC within the MARS implies both signal and physical security:

  --Signal security - Measures intended to deny or counter hostile exploitation of electronic missions on Radio and Internet.
  --Physical security - measures designed to safeguard personnel; to prevent unauthorized access to equipment, installations, material, and documents; and to safeguard them against espionage, sabotage, damage, and theft.

- Many of these concerns either directly or indirectly impact on our Army MARS communications activities.

- Information about military unit strengths, operational capabilities, personal information, deployment intentions, threat condition levels at military/federal installations (THREATCON), or other data related to current operations could provide exploitable information to potential enemies.

- In the wrong hands it can severely impact on our military operations and the lives of our service members. Since the primary means of communication within MARS is electronic, which cannot be totally protected from enemy interception, MARS personnel have the additional responsibility to ensure that information of value to an enemy is not released through ignorance or carelessness. Army MARS operators should always practice continuous OPSEC as follows:

• Our communications and the traffic we relay, either by voice,digitally or by the internet, should neither confirm nor deny, or otherwise include information regarding past, present or future military unit deployments and military operations.

• We should avoid casual conversations regarding military operations.

• Do not speculate about any military course of action. Seemingly harmless information, if combined with other supposedly innocent information, can divulge critical data that could endanger lives and impact mission success. To ensure discussions on our MARS nets do not violate OPSEC some simple and common sense rules apply:

• Identify inappropriate information contained within a message. Do not accept or inject into the MARS system any message that violates the restrictions we have discussed and notify the customer as to the reason the message cannot be sent through the MARS network.

• Be alert for possible unauthorized transmissions and questionable station call signs; report these incidents through your state chain of command to Army MARS headquarters.

• We should avoid casual conversations regarding military operations.

• Do not speculate about any military course of action. Seemingly harmless information, if combined with other supposedly innocent information, can divulge critical data that could endanger lives and impact mission success. To ensure discussions on our MARS nets do not violate OPSEC some simple and common sense rules apply:

• Be alert for possible unauthorized transmissions and questionable station call signs; report these incidents through your state chain of command to Army MARS headquarters.

• **Do not transmit MARS operational frequencies in the clear over the air unless absolutely necessary; instead use authorized alpha character frequency desiccators. Never transmit frequencies and their frequency designator together over the air.**

• If frequencies or desiccators are requested from unknown sources, do not provide the information. Forward any requests through your state chain of command to headquarters for validation.

• You should report suspected violations of good OPSEC practices immediately up your chain of command to the State Director and to the appropriate Area Coordinator or Command Director.

QSL Cards - Army regulations and good OPSEC procedures prohibit military stations from confirming their transmissions on military frequencies.

• The only exception to this policy is the annual Armed Forces Day amateur to military cross-band tests and interaction with amateurs on COMEX exercises, when QSL cards are made available to amateurs.

• Requests for QSL cards for any other operation received by members should be forwarded to Army MARS Headquarters for response.

• This does not preclude in any way the ability of MARS members to continue sending QSL cards for amateur radio service operations conducted on amateur frequencies.

• Members are allowed to display the MARS insignia on their amateur QSL card at their discretion.

Physical Security Measures - Physical security measures you should be concerned with include:

• Your equipment.
• Your station premises.
• Your operational documents and references. Physical security in all three is common sense.
• Equipment. SECURE your equipment, your premises and your documents, both paper and computer disks from access to unknown persons. If your equipment is stolen you will certainly report the theft to the police, but if you have programmed the MARS net frequencies into your transceiver's memories you should also report the loss to Chief, Army MARS (CAM) through your State Director.

• Station premises. Your ATO is in many regards a "little piece" of the U.S. Army and, although unlikely, it is conceivable that it could become the target of terrorists.
• Operational documents. The essential principle of document security is NEVER discard any document which you would want an enemy to have. In other words, treat every MARS document AS IF it were marked FOUO whether it is or not. Here are some disposal methods you might consider:

--Burning (be careful--remember safety!).
--Tearing into small pieces and separate them into two groups, one goes to your garbage can, one to your paper trash or recycling container.
--Shredding. Probably the best way to dispose of these materials is to use a paper shredder. There are many inexpensive models available at discount and office supply stores. With identity theft becoming more prevalent everyone should have one to dispose of any personal records involving sensitive information.

Practical Exercises - Here are some potential scenarios that you may encounter. I'll describe the situation and then we can discuss what you think the correct action might be. Finally, I'll provide you with some thoughts on how each problem could be handled.

Question: Reserve Unit Observations. You noticed last week that the parking lot of the local Army Reserve Unit was full of privately owned vehicles and that the military vehicle motor pool was empty. Today what appear to be spouses of unit members are observed driving the civilian vehicles away. Should you discuss this during on your next MARS net?

Answer: In a word, NO. You would be divulging information regarding a possible troop movement. Enemy intelligence would take this piece of "chatter" and add it to their collection, perhaps helping to complete a "picture" of our intentions and capabilities.

Question: The SWL QSL card. You receive a SWL card from a ham in Portugal asking you to provide a QSL for transmissions he heard on your MARS net. What should you do?

Answer: Again the answer is no. Although at face value confirming this "small" bit of information may seem inconsequential it can be used as a small piece of a big puzzle that could have a significant impact. Instead, send the request to through your chain of command to Army MARS Headquarters, at Fort Huachuca and include as many details concerning the transmissions in question as possible.

Question: The Stranger at a Restaurant. Stopping by a local restaurant for lunch, a passerby notices the MARS decal on your car's windshield. Laughing, he asks, "Are you from Mars?" You explain and he tells you he's a ham operator. He joins you for coffee and you exchange ham radio call signs. He says he'd like to listen to some MARS nets and asks for frequencies and times. What do you say?

Answer: You tell him NOTHING of frequencies and times. These are generally FOUO and individuals outside MARS do not have a need to know. Tactfully dodge the question and explain that MARS is open to amateur operators who are U.S. citizens and invite him to contact your state director for an application to join. Your state director has the authority to selectively include limited frequency/net-time information on recruiting materials to encourage prospective members to monitor net operations.

Question: A member station advises that he's misplaced his frequency matrix and asks you for the frequency in the clear. What do you do?

Answer: Deny the request, as it would require you to associate a designator with its corresponding frequency. At your discretion as NCS, you could appoint him as Alternate Net Control (ANCS), directing that he stay on the primary frequency to acknowledge any latecomers directing them to the alternate frequency. As a practical matter a simple phone call could fix the problem immediately. Remind the member that he can request a new copy of the frequency matrix through his chain of command.

Question: The Emergency Exercise. Your State Emergency Coordinator asks you to draft an on-air emergency communications exercise. You are familiar with the vulnerabilities of your local power system and decide to incorporate them in the scenario. Is this a good idea?

Answer: No. Although this may be considered "open source" information it's disclosure on the air is NOT in the best interests of the security of a critical utility. FOUO Material Disposal.

Question: A message from Army MARS Headquarters directs that a document has been superseded and may be disposed of. It is NOT marked For Official Use Only (FOUO). How do you dispose of the document?

Answer: There has been a lot of discussion over the years about this topic. MARS operators do NOT handle classified information, but the documents in their possession are often sensitive. Asking yourself "Would this old document be of any value to our enemies if they had it?" will

provide the answer. If you hesitate, the answer is probably "Yes". Dispose of it in the same manner you would any FOUO material.

Question: During informal net time, NCS asks your opinion -- as a veteran -- of an ongoing military operation overseas. How do you respond?

Answer: Regardless of your military experience, do NOT offer comments about on-going military operations, no matter where they are taking place; no information can be inadvertently disclosed if you simply say nothing.

Question: The Insurance Agent. While operating on a MARS net, your life insurance agent drops in. You have some FOUO MARS material open at your operating position where you both have just sat down to talk. What do you do?

Answer: Simply discretely close or cover them.