



OFFICE OF THE NATIONAL COMMANDER
NATIONAL HEADQUARTERS
CIVIL AIR PATROL
United States Air Force Auxiliary
MAXWELL AIR FORCE BASE, ALABAMA 36112-6332

4 Nov 2009

MEMORANDUM FOR ALL REGION AND WING COMMANDERS


FROM: HQ CAP/CC

SUBJECT: INTERIM CHANGE LETTER – CAPR 100-1 VHF-FM Encryption Policy

1. This interim change to CAPR 100-1 provides initial guidance for the planning and preliminary use of encryption within the CAP communications system. Many procedures and standards that would be required for full implementation of encryption remain to be developed. However, tasking agencies are already requesting CAP use of encryption on selected missions. Therefore, this interim policy begins the process of addressing the complex issues surrounding encryption.
2. As CAP's missions transition further into the realm of sensitive and possibly even classified taskings, the issue of communications encryption becomes crucial. CAP-USAF has verified that DoD and AF policy guidance on encryption applies to CAP. When the narrowband transition is complete, with all repeaters installed and all radios reprogrammed, the repeater system and the majority of the ground-based VHF-FM radios will be capable of encryption IAW DoD policy. Aircraft readiness to support encryption will take longer to implement, but options are currently being reviewed. Identified requirements and priorities for encryption will be addressed as required funds become available.
3. Pending further development of implementation procedures, CAP will comply with the following requirements:
 - a. CAP encryption implementation must be IAW AFI 33-201 Vol. 1 using NIST-validated equipment with current FIPS 140-2 certificates.
 - b. CAP must be prepared to use encryption IAW tasking agency requirements.
 - c. Before routine use of VHF-FM encryption will be possible, CAP NHQ and CAP-USAF must develop procedures for secure distribution and storage of encryption keys. Communications managers must take into consideration the possibility of secure communications as a mission requirement in the near future and plan accordingly.
 - d. Customer requirements for encryption may limit the usefulness of non-encrypted radios on AF assigned missions and some corporate missions, and communications managers must assign resources accordingly with this in mind. We anticipate that non-encrypted radios will still be useful for many support roles and most non-mission communications.
 - e. Systems used to interconnect repeaters and remote base stations must support encryption at all times. Effective immediately, any new system of this type must automatically retransmit original encrypted signals without unsecure intermediate decrypting and re-encrypting. In other words, signals that were originally encrypted may not be passed through unsecured networks unless preserved in their original encrypted form. Existing systems must be brought into compliance by 31 December 2012.

f. CAP NHQ will take steps to upgrade the VHF-FM radios in the CAP aircraft to provide the necessary encryption capability as quickly as possible.

4. This policy is effective immediately and will be included in the appropriate regulations as soon as practical. Thank you for your support and assistance in implementing this Air Force mission requirement.


AMY S. COURTER
Major General, CAP
National Commander

cc:

CAP/CV/CS/EX/MD/FM/LG/XP/GC/EXM/EXS

Col Skiba

Col Guimond

CAP Communications Team Leader

CAP Region Director of Communications

CAP Wing Director of Communications

CAP Wing Administrators

CAP-USAF/CC/CV/XO/LG/FM/JA

CAP-USAF Region Commanders

CAP-USAF State Directors