



**UNITED STATES MARINE CORPS**  
MARINE AIR GROUND TASK FORCE TRAINING COMMAND  
MARINE CORPS AIR GROUND COMBAT CENTER  
BOX 788100  
TWENTYNINE PALMS, CALIFORNIA 92278-8100

3000  
7E

JAN 13 2010

POLICY LETTER 1-10

From: Commanding General  
To: All Hands

Subj: ANTITERRORISM AND FORCE PROTECTION (AT/FP) POLICY

This policy highlights basic AT/FP practices and reporting mechanisms in order to provide the best security possible to the service members and their families associated with Marine Air Ground Task Force Training Command and Marine Corps Air Ground Combat Center, Twentynine Palms (MAGTFTC, MCAGCC).

Antiterrorism is defined as "defensive measures used to reduce the vulnerability of individuals and property to terrorist acts." Force protection describes "preventive measures taken to mitigate hostile actions against Department of Defense (DoD) personnel (including family members), resources, facilities, and critical information."

With the War on Terror and the potential of adversary and criminal behavior directed against MAGTFTC and MCAGCC personnel, I expect all hands (military, civilians, and dependents) to be vigilant regarding force protection and potential acts of terrorism. One of the most important individual protective measures DoD-affiliated persons can take is to develop personal habits and practices that frustrate terrorist attempts.

These include the following:

1. Keep a low profile.
2. Be unpredictable.
3. Guard information.
4. Be alert for anything suspicious or out of place.
5. Be alert to strangers who are on government property for no apparent reason.
6. Keep associates and family members informed of leave and liberty plans.
7. Do not disclose information to strangers regarding family travel plans, troop movements, or security measures and procedures - think before you post anything on social media websites.

Additionally, I expect all hands to know and practice their security responsibilities and Operational Security (OPSEC) protective measures to become a "hard target." By using secure and encrypted communications, controlling access to computer networks, destroying unnecessary personal and work-related papers, concealing operational indicators, and varying routes and activities, we will collectively protect the critical information our adversaries require to plan and execute terrorist activities.

Subj: ANTITERRORISM AND FORCE PROTECTION (AT/FP) POLICY

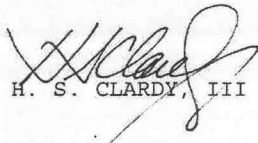
Antiterrorism and force protection are command responsibilities. Practicing each makes you a "hard target." I expect commanders, at all levels, to brief personnel and family members under their charge on personal security and safety procedures. AT/FP is accomplished through a systematic approach which integrates the planning and application of combating terrorism, physical security, OPSEC, and personal protective measures, supported by intelligence, counterintelligence, and other security programs.

We have multiple programs and initiatives that go a long way in securing our installation and our families. Random Antiterrorism Measures (RAM) are random, multiple security measures that consistently change the look of an installation's force protection program. Conducting RAM can be an inconvenience at times, but a necessary inconvenience and a vital part of our overall security posture. Personnel may experience delays while law enforcement personnel exercise the RAM program.

Eagles Eyes, an installation and community watch program emphasizing community awareness and involvement, was established in 2002. Additionally, Eagle Eyes helps prevent or reduce terrorist threats by educating the community on what to look for as well as how and where to report suspicious activity. Suspicious behavior includes:

1. Surveillance. Are you aware of anyone recording or monitoring activities, taking notes, or using cameras, cell phones, maps, binoculars, etc., near a military facility?
2. Suspicious Questioning. Attempting to gain information in person or via phone, mail, e-mail, etc., regarding deployment status of units or personnel.
3. Tests of Security. Attempts to penetrate or test physical security or procedures at a military facility.
4. Acquiring Supplies. Attempts to improperly acquire explosives, weapons, ammunition, dangerous chemicals, uniforms, badges, flight manuals, access cards, or identification that could be used in a terrorist or criminal act.
5. Suspicious Persons. Anyone who does not appear to belong in the workplace, neighborhood or business establishment near a military facility.
6. Dry Runs. Behavior that appears to be preparation for terrorist activity, such as mapping out routes, playing out scenarios with other people, monitoring military facilities, timing traffic lights or traffic flow, or any other suspicious activities.
7. Deploying Assets. Abandoned vehicles, stockpiling of suspicious materials, or persons being deployed near a military facility.

You are the first line of defense for our antiterrorism and force protection programs. We know who or what belongs and we know what does not belong in our neighborhoods or work centers. The simple act of recognizing suspicious behavior and reporting it to authorities could thwart terrorist attacks and save lives. Report any suspicious behavior to military or civilian police, the Eagle Eyes Program hotline 760-830-EYES (3937), or your chain of command as soon as possible.

  
H. S. CLARDY, III