



UNITED STATES MARINE CORPS

3D MARINE DIVISION (-) (REIN), FMF
UNIT 35801
FPO AP 96602-5801

IN REPLY REFER TO:
DivO 3850.3B
G2
23 MAY 1994

DIVISION ORDER 3850.3B

From: Commanding General
To: Distribution List

Subj: GUIDANCE FOR COUNTERINTELLIGENCE GARRISON RESPONSIBILITIES

Ref: (a) MCO 3850.1G, Policy and Guidance for Counterintelligence Activities
(b) FMFM 3-25, Counterintelligence
(c) SECNAVINST 3820.2D
(d) OPNAVINST 5510.1H
(e) DivO P5510.9K, SOP for IPSP
(f) DivO P5040.3D, SOP for Command Readiness Evaluation Program
(g) DivO P3800.1K, Division Intelligence SOP

1. Purpose. To provide regimental and battalion commanders guidance and direction for the accomplishment of their counterintelligence (CI) garrison responsibilities in accordance with reference (a), and as promulgated by references (b) through (g).

2. Cancellation. DivO 3850.3A.

3. Information

a. Definition. Counterintelligence is that aspect of intelligence activity which is designed to discover, neutralize, or destroy the effectiveness of actual or potential hostile intelligence activity, and to protect information from hostile espionage, individuals from subversion and terrorism, and installations or material from sabotage.

b. Doctrine. Basic doctrine and guidance for the conduct of active and passive CI operations in combat and garrison are contained in references (b) and (g). Passive CI measures enhance the security of the command and deter the inadvertent disclosure or compromise of classified information. This order concerns itself with peacetime garrison responsibilities. Commanding Officers, general and special staff officers and other supervisory personnel are encouraged to use locally available CI assets to the fullest extent possible.

c. Jurisdiction. In garrison, exclusive jurisdiction for matters involving actual, potential or suspected sabotage, espionage and subversion, including actual, suspected or attempted defections, rests with the Naval Criminal Investigative Service (NCIS). Reference (c) provides specific guidance.

d. Organization

(1) 3d Marine Division Security Manager. The Security Manager (AC/S, G-2) for the Division exercises staff cognizance over the Information and Personnel Security Program for all units assigned to the Division. As the AC/S, G-2, he is responsible for providing counterintelligence assistance to all subordinate commands if requirements exceed their capabilities.

(2) On-island CI Teams are administratively controlled by the Commanding Officer, Intelligence Company, 3d Surveillance Reconnaissance Intelligence Group (3d SRIG). The AC/S, G-2 (SCIO), III MEF has operational control of all CI activities. Division units receive CI support from the 3d CI Team. Direct liaison between 3d CI Team (CIT) (623-4700/4553) and Regimental and separate Battalions S-2 officers is authorized and encouraged for routine garrison support. Requests for exercise support will be submitted in writing via the chain of command.

e. Intelligence Oversight. Commanders will ensure compliance with reference (c) regarding the Department of the Navy's investigative and counterintelligence collection and retention guidelines. Reference (c) provides general policy, limitations, procedures and operational guidance pertaining to the collection, processing, storage and dissemination of information concerning U.S. persons and organizations not affiliated with the Department of Defense (DOD). Particular attention should be given to authorized/prohibited information gathering activities and retention criteria. Additional guidance concerning Intelligence Oversight is contained in current edition of reference (c).

f. Credentials. Counterintelligence credentials are issued by Headquarters, U.S. Marine Corps, to authorized Marines assigned to CI billets. Credentials identify those personnel accredited and authorized to conduct CI activities within the DOD. Counterintelligence personnel have been the subject of Special Background Investigations; therefore, they have a Top Secret clearance and the access required for the performance of their duties. Counterintelligence personnel will display credentials upon request while conducting CI activities within the division. Division personnel will render assistance for the accomplishment of assigned CI missions. Reference (a) sets forth responsibility for the proper use of credentials.

g. Clothing. Civilian clothing may be worn by CI personnel while conducting official business in accordance with reference (a).

h. Counterintelligence Services. Counterintelligence services are available to any division unit upon request. Requests for CI services should be forwarded to the Commanding General (AC/S, G-2) for validation and coordination with III MEF, 3d SRIG, Intelligence Company and 3d CI Team. Direct liaison between units/sections and 3d CI Team is authorized and encouraged. Instructions contained herein will be observed.

(1) Counterintelligence Survey. The CI survey is a service designed to assist commanders in establishing systems, procedures and safeguards to protect military installations against sabotage, and to protect personnel and organizations from the threat of espionage, subversion and terrorism. The CI survey will establish, rather than test, compliance with existing security requirements. Paragraph 8002, reference (b), provides detailed guidance regarding the purpose and conduct of the CI survey.

(2) Counterintelligence Evaluation. The Counterintelligence Evaluation (physical security) is similar to the CI survey, is limited in scope, and will satisfy requirements for ensuring compliance with existing security regulations. The evaluation involves specific aspects of the storage of classified material within a unit. Requests for a CI evaluation will identify the storage area locations and a unit point of contact in accordance with reference (e). The request will be forwarded to the Team Commander of the supporting CI Team via the Commanding General (Attn: Security Manager), 3d Marine Division.

(3) Unannounced Counterintelligence Inspections. Unannounced CI Inspections are conducted by CI personnel to determine compliance with Information and Personnel Security Program regulations (references (d) and (e)). The purpose of this type of inspection is to determine whether classified material is properly protected. Classified material includes items which are used to produce classified documents, e.g., scratch/carbon paper, drafts, typewriter ribbons and word processor diskettes. Hazards or potential hazards (e.g. unlocked windows/doors, lack of double-check on security containers, etc.) will be identified and recommendations provided to ensure in-depth security is achieved.

(a) Frequency. Counterintelligence personnel conduct periodic, unannounced inspections of all Division units and sections that use and/or store classified material or equipment. Each unit or section will be inspected at a minimum of once during each quarter, normally during non-duty hours. The Security Manager will schedule unannounced inspections and coordinate their conduct with the Team Commander, 3d CI Team. Results of quarterly unannounced security inspections will be provided to the Division Security Manager by the CI Team, who will forward by endorsement the report to the inspected unit's commanding officer.

(b) Guidance

1 When counterintelligence personnel arrive at the unit/section to be inspected, credentials will be presented upon request to duty personnel and the purpose of the inspection will be explained.

2 The inspection team's senior member will normally request that a command representative accompany and observe the inspection party. It is preferable that this representative be an officer or a staff noncommissioned officer.

3 The inspection will be sufficiently detailed to ensure compliance with current directives. Locked containers (e.g. file cabinets, desks) not designated for the storage of classified material may be opened by the inspectors and the contents inspected. Such containers will be opened with a key or by a competent technician (i.e., CI personnel who are schooled in Defense Against Methods of Entry (DAME) or who have had locksmith training).

4 If classified material is found adrift, it will be turned over to the unit's security manager or his designated representative. The representative will sign a receipt for the material and ensure that it is properly safeguarded. If during the inspection, security containers, strong rooms or vaults are discovered unsecured and unguarded, the unit representative will recall responsible personnel and require that they conduct a complete inventory of its classified material (reference (e) applies). A reinspection will be conducted within 30 days if a security violation was found during the course of an unannounced CI inspection.

5 Unit duty personnel will be briefed upon the conclusion of the inspection.

(4) Vacated Command Post Inspection (VCPI). All units or sections are responsible for the protection of classified material and military information in both tactical exercise and garrison environments. Commanders will ensure that the area is inspected for any military information left adrift prior to departing the area. Counterintelligence personnel may conduct VCPI's to ensure that classified material or unclassified information of an intelligence value has not been left adrift. Requests will be submitted to the CI Team providing support via the Commanding General (Attn: Security Manager), 3d Marine Division or the appropriate field commander with attached CI elements. When feasible, requests should be in writing and provide eight digit coordinates or building numbers of each location; however, verbal requests will be accepted by the supporting CI Team on a case by case basis. VCPI's are not routinely conducted of rotational battalion headquarters buildings since the advance party of the replacing battalion will occupy the building prior to the departure of the relieved battalion.

(5) Announced Inspections. These inspections consist of Functional Area Inspections (FAI) and Staff Assistance Visits (SAV), and are provided to assist commanders in determining their compliance with existing Information and Personnel Security Program Management and CI regulations. A FAI or SAV inspection may be requested, but normally will be scheduled in accordance with reference (f). Written SAV inspection results will be submitted only when a "Not Mission Capable" inspection grade is warranted. FAI results will be forwarded via the appropriate chain of command. The conduct of either inspection does not relieve the unit security manager of his responsibilities to conduct and make a record of his own inspections as established by reference (d) and (e). Reference (e) contains the Information and Personnel Security Program Management checklist which is used by the Division Security Manager's office for conducting SAVs and FAIs.

(6) Penetration Inspections. A penetration inspection provides a realistic test of an installation's or unit's security measures. The inspection is conducted in such a manner that personnel, other than the unit commander and those personnel he desires to notify, are unaware that such action is taking place. Additional information concerning penetration inspections is contained in paragraph 8002.h of reference (b). Requests for penetration inspections will be submitted in writing by unit commanders to the Commanding General (Attn: AC/S, G-2), 3d Marine Division. The need of this type of inspection must be carefully considered and have the concurrence of the requesting unit commander, the Division Security Manager and supporting CI team commander. Paragraph 8002.h.(1) through (5) of reference (b) must be carefully considered during the planning and execution of a penetration inspection.

(7) Counterintelligence Investigations. Counterintelligence personnel coordinate with the local Naval Criminal Investigative Service (NCIS) in matters involving the investigation of actual, potential or suspected espionage, subversive and terrorist activity, and defections. Unit commanders will conduct preliminary inquiries into the potential or suspected compromise of classified material in accordance with references (d) and (e). Counterintelligence personnel may conduct a preliminary investigation, with concurrence of NCIS and when directed, in accordance with limitations addressed in references (a) through (e).

(8) Technical Assistance. Counterintelligence personnel can provide limited technical assistance for those areas discussed below.

(a) Repair and maintenance of security containers will be performed by the MCB Butler Facilities Maintenance locksmith upon request. Technical assistance and instruction related to security containers, vaults, lock and padlock mechanisms used for storage of classified material are available from CI personnel. Routine combination changes and preventive maintenance, not to include the lubrication of the lock mechanism, is the user's responsibility. Counterintelligence personnel are available to instruct personnel on how to change combinations and determine the course of action required to affect possible repairs to damaged security equipment. Direct liaison with 3d CI Team for combination change procedure classes is authorized and encouraged.

(b) Technical Surveillance Countermeasures (TSCM) inspections may be required for specific areas in the Division. Additional information is contained in the current editions of MCO 5511.11 and ForO 5511.5. Guidance concerning TSCM inspections is available from the Division Security Manager or Team Commander, 3d CI Team. This type of inspection will not be discussed on unsecured telephone or in unclassified correspondence when specifics are identified (i.e., locations, time frame of the inspection and type of classified information to be protected). Additionally, TSCM inspections shall not be discussed in those areas to be inspected or in those areas that have been inspected.

(9) Security Education and Training. Unit security managers and intelligence officers must provide security indoctrination briefs and periodic training to all personnel. Local threat briefings are required at least once every three years and must be coordinated with the local NCIS through the Commanding General (Attn: Security Manager), 3d Marine Division. Reference (e) establishes Division policies for security education. The CI Teams can provide CI related classes and lectures as requested. Unit commanders are encouraged to request CI training assistance as needed. Requests will be submitted to the supporting CI Team via the Commanding General (Attn: Security Manager), 3d Marine Division, at least three weeks in advance. These must indicate the subject(s) desired (specific topics and objectives), approximate number of officers/enlisted personnel to attend, location of the classroom, date/time desired and a point of contact. Direct liaison with the 3d CI Team is encouraged prior to requesting a class to ensure that times and dates are supportable.

(10) Information and Personnel Security Program. Counterintelligence personnel can provide guidance and interpretation of references (d) and (e) upon request to security managers and assistants, and those personnel having custodial responsibilities for classified material.

(11) Operation Security (OPSEC). Counterintelligence can assist the commander in formulating and implementing his OPSEC responsibilities in garrison as well as in a tactical environment. Since the operations officer (G-3/S-3) assists the commander in the overall planning and executing of operations, he has primary supervisory responsibility for OPSEC functions. Counterintelligence personnel can provide the commander with information or area briefings concerning actual or potential hostile intelligence collection threat, unit vulnerability assessments to these, and recommendations regarding viable OPSEC measures to counter these.

(12) Pre-Construction Technical Assistance. This service consists of rendering security advice during the planning phase of new construction, modification, alteration or additions to areas used to secure classified/sensitive information. It is designed to ensure that all aspects of technical and physical security are considered in this planning to avoid costly modification of security features after the work has been completed and to ensure that required security measures have been incorporated. Requests for CI assistance will be submitted to the supporting CI Team via the Commanding General (Attn: Security Manager), 3d Marine Division.

(13) Automatic Data Processing (ADP) Security. Computers and word processors operate in an environment that must be considered hostile and are inherently vulnerable. Due to the wide range and rate of growth of applications and the increased dependence on such systems, it is imperative that security aspects be considered. Security vulnerabilities can be solved, or at least reduced to an acceptable level of risk, by developing an effective security program. Commanders must take adequate measures to identify potential vulnerabilities in classified and unclassified ADP environment. Policy and guidance for ADP security is contained in the current editions of OPNAVINST 5239.1, MCO P5510.14 and reference (e).

(14) Terrorism Threat

(a) The threat of violence as an expression of political motivation is not new. However, the form and degree of the acts of violence and the organized scale that is surfacing internationally continually changes. Terrorist groups capitalize on the human concerns of people and nations by the commission of atrocities and violent acts for political recognition and the furthering of their goals. Typically, their goals are placed well above the respect for human life. In most cases, the terrorist will be rational, intelligent, calculating, motivated, well disciplined, very united and in good physical condition. Normally, terrorists do not have strong desire to survive, their planning is calculated and their equipment is usually more than adequate.

(b) Counterterrorism policy and procedures for all Marine commands is contained in MCO 3302.1. In addition, on Okinawa the Commanding General, Marine Corps Base Camp Butler, has overall responsibility for Counterterrorism actions (refer to BO P3850.1A for details).

(c) Commanders must ensure that personnel are aware of the potential threat in Okinawa and other areas that may be visited during training, and that they take appropriate measures to reduce their unit's vulnerability to a threat. In addition, terrorist threat and awareness briefings may be requested from the Naval Criminal Investigative Service, Okinawa, or the 3d CI Team, via Commanding General (Attn: AC/S, G-2), 3d Marine Division.

(15) Counterintelligence in Exercises. Where practical, counterintelligence personnel should be integrated into regimental sized or larger training exercises. This can be accomplished by involving CI representative in the planning phase, thus integrating CI scenario items in the overall exercise evolution. Combat CI functions and capabilities in support of a unit are outlined in references (b) and (g). Requests for CI support for training exercises must be justified and forwarded to the Commanding General III MEF, via the Commanding General (Attn: AC/S, G-2), 3d Marine Division, early in the planning phase (30-45 days prior to exercise dates).

4. Action. Commanding Officers will:

a. Initiate those CI measures necessary and required to ensure the security of their unit. Maximum use of available CI support is encouraged.

b. Issue instructions to ensure prompt reporting and handling of any actual, attempted or suspected sabotage, treason, sedition, subversion, terrorism, defection or security violation. These incidents should be reported by the most expeditious means, consistent with security, to the Commanding General (Attn: Security Manager).

c. Ensure that appropriate duty orders contain reporting and notification procedures in those cases listed in paragraph 4b above. Additionally, duty orders shall include specific guidance for the recognition of CI credentials and assisting CI personnel conducting their assigned mission.

d. In cases of actual, attempted or suspected sabotage or espionage, every effort will be made to preserve the condition of the site. Guards will be posted to prevent tampering or handling of physical evidence. The Naval Criminal Investigative Service will be notified immediately of any incidents, as described in paragraph 4.b above, requiring their attention. In addition, during working hours the Division Security Manager or AC/S, G-2 will be notified of the incident; after working hours, the III MEF/Division Command Duty Officer will be advised of the incident by telephone, and will in turn notify the Division Security Manager and/or AC/S, G-2.


P. V. KELLY
Chief of Staff

DISTRIBUTION: A/D

Copy to: CG, III MEF (SCIO) (1)
TmCmdr, 3d CI Team (5)