UNITED STATES MARINE CORPS
I MARINE EXPEDITIONARY FORCE
U.S. MARINE CORPS FORCES, PACIFIC
BOX 555300
CAMP PENDLETON, CALIFORNIA 92055-5300

I MEFO 5511.2F
G-2

FEB 25 2011

I MARINE EXPEDITIONARY FORCE ORDER 5511.2F

From: Commanding General
To: Distribution List

Subj: TECHNICAL SURVEILLANCE COUNTERMEASURES (TSCM) PROGRAM

Ref: (a) SECNAVINST 5500.31A
(b) DCID 6/9
(c) SECNAVINST 5510.36
(d) DoDINST 5240.05M (C)
(e) DODINST 5204.05
(f) MCO 5511.20
(g) Tri-Service Agreement for TSCM of 6 May 98
(h) Telephone Security Group (TSG) Guider, 1 through 8

Encl: (1) Procedures in the Event of Detection of Suspicion of A Technical Penetration
(2) TSCM Suppor Request Guidelines
(3) Definitions

1. Situation.

a. The primary purpose for the TSCM Program and TSCM support is to preclude clandestine surveillance in sensitive areas where classified information is routinely discussed or processed . The Marine Corps possesses an organic TSCM capability to provide commanders with secure facilities for planning and controlling tactical operations, secure communications, and to augment counterintelligence special operations.

b. Historically, foreign intelligence services employ technical surveillance devices in espionage operations directed against U.S. personnel and installations both in the United States and abroad. The protection of classified and sensitive information from technical surveillance is the responsibility of every commander. In today's high technology environment, the availability of technical surveillance equipment is such that virtually any foreign intelligence, terrorist, or dissident group can acquire and employ technical surveillance against Marine Corps assets.

2. Cancellation: I MEFO 5511.2E.

3. Mission. In order to provide guidance for the management of

the I MEF TSCM program. Technical Surveillance Countermeasures (TSCM) surveys and inspections can reduce the likelihood of a technical penetration. The TSCM Program is an augmentation to the command's overall security program and is designed to detect, isolate and nullify the presence of technical surveillance operations. TSCM surveys will identify technical security hazards and vulnerabilities which may lead to a technical penetration. Lastly, TSCM personnel provide education to commanders, at all levels, concerning the potential technical surveillance threats in their Area of Operations.

4. Execution.

a. Justification and Selection of Spaces Requiring TSCM Support. Specific criteria is used to select spaces and facilities requiring TSCM support. The following criterion determines TSCM support requirements:

(1) Basic Criteria. Request TSCM support for those spaces in which discussions at the Secret level or above routinely take place. Such spaces must also afford continuous 24 hour access control to maintain the validity of the TSCM survey. Reference (a) contains criteria for justification of TSCM support within the Department of the Navy and Marine Corps. References (b) and (c) contains guidance relative to physical security matters.

(2) Executive Level Offsite/Classified Discussions. TSCM support to in-conference monitoring may be requested for conferences and other such meetings of a classified nature. Sufficient personnel access controls and physical security measures are essential; without them, TSCM support services may foster a false sense of security. TSCM support to in-conference monitoring provides technical surveillance countermeasures for the duration of the conference. Access to the meeting space is needed at a minimum of eight (8) hours prior to the start of the meeting and for the duration of support. Requesting units are required to provide proper security to the meeting location once TSCM services have started.

(3) New/Renovated Facilities. New installations or spaces having undergone major renovations will not receive TSCM support until all construction is completed, the spaces are manned, fully operational, and security measures are implemented.

(4) Pre-Construction Assistance. Future construction concerning a facility identified to process Secret or above information qualifies for TSCM pre-construction assistance. Pre-construction assistance is encouraged to ensure the security standards are incorporated into construction or modification

plans and technical surveillance devices are not emplaced during construction.

(5) Automobiles, Ships, and Aircraft. TSCM support for Flag Officer/General Officer level automobiles and aircraft can be conducted upon approval from the AC/S G-2, I MEF. TSCM support for ships will not be conducted unless justified by extraordinary circumstances (see reference (a), paragraph 6.a.5 pertains).

(6) Information systems. Areas which routinely process classified or sensitive information utilizing computerized systems justify TSCM support. TSCM practitioners are trained to locate, identify and neutralize covert channel communications. TSCM personnel are trained to address unique security concerns not covered by network administrators. Counterintelligence measures can be recommended to enhance the security of digital information from threats such as hacking, phreaking and foreign intelligence exploitation.

(7) Additional Areas. Other sensitive spaces exist within the Marine Corps which may be vulnerable to technical surveillance and require TSCM support. Support for these areas will be on a case-by-case basis as warranted by the threat to the sensitive area.

b. Recurring Support. No facility qualifies automatically for recurring TSCM support. Once an area has been subjected to a fully instrumented survey, the results are valid as long as the security integrity of the facility is maintained. Consideration for recurring service will be based upon the following criteria:

(1) Evidence suggesting an area has been technically penetrated.

(2) Extensive construction, renovation, or structural modifications requiring unescorted access by un-cleared individuals.

(3) Unauthorized personnel have gained uncontrolled access to the facility.

c. TSCM surveys will be conducted in accordance with references (a), (d), (e) and (f). TSCM Personnel shall also evaluate the applicable spaces for technical and physical security vulnerabilities and, when necessary, provide recommendations to eliminate any security deficiencies identified.

5. Administration and logistics.

a. Request Procedures.

(1) Submit all requests from I MEF major subordinate reference (a). G-2/Staff Counterintelligence Officer (SCIO) will provide guidance on TSCM matters to requesting organizations as required.

(2) Upon validation of requirements by the I MEF (AC/S) G-2, the TSCM Team will be tasked with providing the requested support. Due to the limited distribution nature of TSCM requests, the TSCM Officer-in-Charge will provide a copy of the request to the Commanding Officer, CI/HUMINT Support Co for further coordination with 1st Intelligence Battalion.

(3) Upon receipt of validated tasking, I MEF TSCM OIC will coordinate with the SCIO to prioritize and schedule TSCM support. First priority will be to Operating Force commands, followed by Marine Corps supporting establishments, and commands of other services. Second priority will be to provide TSCM services and support to non- Operating Force commands when requested by the Marine Corps TSCM Program Coordinator, Marine Corps Intelligence Activity, Commander, Naval Criminal Investigative Service (NCIS), or local Resident Agent in Charge (RAC), in accordance with reference (g).

(4) The I MEF TSCM Team has direct liaison authority with Marine Corps TSCM Program Coordinator, Marine Corps

Intelligence Activity and Commander, NCIS (Code 0024B5) on TSCM technical and equipment matters.

(5) Requests for TSCM support will not be conveyed over unsecure channels or telephones located in any location pending or scheduled for TSCM support, in accordance with paragraph 6.c of reference (a). Should a command discover a clandestine surveillance device, follow the guidance in enclosure (1). To request TSCM support, follow the guidance in enclosure (2).

b. TSCM Personnel and Training.

(1) Per reference (d), only Department of Defense (DOD) certified TSCM specialists will conduct TSCM services. The nature of TSCM, as a specialized counterintelligence function, requires personnel who possess extensive knowledge in investigative, electronic, and construction skills. This combination of talents is necessary to successfully conduct the complex and detailed operations associated with TSCM services.

(2) I MEF TSCM/Technical Service practitioners shall receive, at least annually, refresher or other specialized training to remain proficient, and knowledgeable concerning technical

penetrations and detection techniques, in accordance with reference (d).

c. Operational Security (OPSEC).

(1) TSCM services are specialized counterintelligence investigations and as such, are particularly vulnerable to compromise. All commands which receive TSCM services must implement OPSEC measures to ensure the success of the countermeasures effort. Assume, until the survey indicates otherwise, that a technical surveillance device is actually in place.

(2) Should discussions concerning pending support take place within the space, the device would most likely be removed prior to the survey and later reinstalled, or simply deactivated remotely. Under such circumstances, the probability of locating a technical surveillance device is diminished greatly. For this reason, no discussion or verbal comments concerning pending TSCM support shall take place in the spaces of concern, nor shall discussions or verbal comments take place during the survey. If a compromise occurs, TSCM specialists will immediately terminate the provided support and report the circumstances which compromised the TSCM support to the I MEF G-2.

(3) Telephone requests or discussions of scheduled TSCM support are considered compromising unless conducted over secure voice systems outside the facility to be serviced. Similarly, e-mail messages referencing anticipated or occurring TSCM services originating from or going to the concerned spaces will also be considered a compromise of the services. The compromise of pending or ongoing TSCM support is a serious security violation and will be reported in accordance with the procedures outlined in reference (c).

d. Reporting.

(1) Results of TSCM services conducted for I MEF Major Subordinate Commands will be reported to the requesting command, via the CG, I MEF. Results of TSCM support conducted for non-FMF commands will be reported to the requesting command via the CG, I MEF and TSCM Program Coordinator, Marine Corps Intelligence Activity. Reports shall be forwarded to the requester no more than 10 working days after the completion of services, per reference (d).

(2) All TSCM service and feedback reports from the serviced agencies, in addition to any Component reporting requirements, will be entered into the designated CI information system and the Technical Security Portal (TSP), as appropriate.

(3) Technical Penetration and Technical Hazard reporting will be conducted in accordance with references (d) and (f).

(4) All requests, validations, and reporting will be forwarded to Marine Corps TSCM Program Coordinator, Marine Corps Intelligence Activity.

(5) The TSCM OIC is responsible for providing copies to the I MEF Counterintelligence/HUMINT Intelligence Office, for the purpose of archiving and maintaining all records relating to TSCM. These records include, but are not limited to TSCM requests, validations, survey results, training and equipment.

e. TSCM Equipment handling and shipping. Budgeting for TSCM equipment procurement is the responsibility of the TSCM Project Officer at MARCORSYSCOM. TSCM equipment shall be kept current to meet the existing threat due to ever changing technology. Equipment needing repairs beyond the scope of local capabilities will be forwarded to U.S. Army Material Command, Intelligence Material Directorate, Fort Belvoir, Virginia. TSCM equipment should be shipped via Defense Courier Service.

6. Command and signal. The Commanding General (CG), I MEF, through the Assistant Chief of Staff (AC/S) G-2, has operational control of the I MEF TSCM Program.

a. Assistant Chief Of Staff, G-2/ Staff Counterintelligence Officer, I MEF. Exercise overall staff cognizance for the TSCM program within I MEF and validate all TSCM requests.

b. Senior Marine Corps Counterintelligence Officer/Enlisted assigned as Counterintelligence/Human Intelligence Officer (CIHO), I MEF.

(1) Act as the focal point between the requesting commands and the supporting TSCM element.

(2) Advise the I MEF Commander on the conduct of TSCM activities in accordance with this order and the references.

(3) Assist the commander and command security manager with security measures that will afford the TSCM service protection from compromise.

c. Commanding Officer, 1st Intelligence Battalion.

(1) Ensure administrative and logistical support is provided in accordance with criteria established by this order, reference (f) and applicable guidance.

(2) Budget for annual TSCM refresher training.

d. Counterintelligence/HUMINT Company Commander.

(1) Provide trained personnel for TSCM support upon direction.

(2) Budget for TSCM expendable supplies.

e. TSCM Officer-in-Charge.

(1) Coordinate and conduct TSCM operations in support of I MEF, in accordance with this order and the references.

(2) Provide TSCM threat data to the Commanding General, I MEF via the CIHO and ACS/G2.

(3) Coordinate TSCM training with the CI/HUMINT, Company Commander.

(4) Conduct liaison with Marine Corps TSCM Program Coordinator, Marine Corps Intelligence Activity on TSCM annual training, equipment maintenance and supply matters.

G. M. RYAN
Chief of Staff

Distribution:List II
Copy to:

Procedures in the Event of Detection or Suspicion of a Technical Penetration

1. Should a command discover an actual or suspected clandestine surveillance device, take the following actions:

a. Secure the area to preclude removal of the device.

b. Conduct no discussions of the discovery within the space where the device was found.

c. Make no attempts at removal of the device.

2. The command will report the discovery immediately to the AC/S G-2, I MEF by immediate precedence SECRET message or other secure means. Do not discuss the matter over unsecure telephones or telephones located in the space where the device was found. The report should include the following information:

a. Time and date of discovery.

b. Area, installation, or facility involved.

c. Specific location within the facility where the device was found.

d. Identity of device by type (e.g. wire, microphone, modified telephone, RE transmitter, etc.) if known.

e. Method and circumstances of discovery.

f. Name and any additional identifying information of the individual who discovered the device.

g. Estimate as to whether the hostile intelligence service was alerted to the discovery.

3. Information concerning the discovery of an actual or possible penetration shall not be released to other persons until authorized by the CG, I MEF.

TSCM Support Request Guidelines

1. Forward all requests for TSCM support within I MEF to the AC/S G-2 for validation and subsequent referral to I MEF TSCM OIC for action. By 1 December each year, Major Subordinate Commands are requested to identify those facilities requiring TSCM support for the coming calendar year.

2. In accordance with OPNAVINST 5510.4B, classify all requests for TSCM support SECRET//NOFORN.

3. All requests for TSCM support should include the following information:

a. Type of support requested (e.g. TSCM survey, TSCM inspection, in-conference monitoring, pre-construction assistance, etc.).

b. Complete identification of the area requiring support, to include name of the facility, room number, and address.

c. Square footage of the area.

d. Identity and telephone number of the command point of contact.

e. Date and serial number of last TSCM report, if any.

f. Clearance requirements for TSCM support personnel.

g. Requests from outside Camp Pendleton must be funded by the requesting unit; therefore, requests must include appropriation data for travel claim purposes. I MEF TSCM personnel will make every effort to procure military airlift and lodging aboard the supported base. Requesting units must plan for per diem for three personnel and a rental van for transporting equipment at the remote location. In some cases, this will necessitate prior planning by the requesting unit in order to put these additional funds in their yearly budget.

Definitions and TSCM Support Available

Technical Surveillance. The use of optical, audio, or electronic data monitoring devices against a target area for the purpose of surreptitiously collecting information.

Sensitive Facility. A facility or area where SECRET or TOP SECRET information is routinely (daily) discussed or processed electronically.

Technical Surveillance Penetration. The deliberate emplacement of an optical, audio, or electronic data monitoring device or the exploitation of existing technical security hazards or weaknesses.

Technical Security Hazard. A condition which could permit the technical penetration of an area through building design or from equipment, which by reason of its normal design, installation, operation, or damaged condition, allows the unintentional transmission of sensitive information outside the sensitive facility's perimeter.

Technical Security Weakness. A defect in the security of a sensitive area which would permit either access by uncleared personnel or aid in the installation of a technical surveillance device.

TSCM Survey. A CI investigation which encompasses a complete electronic, visual, and physical evaluation of a sensitive area by certified TSCM personnel to ascertain that the area is free of technical penetrations and to detect technical security hazards and weaknesses.

TSCM Inspection

(1) The evaluation of a sensitive facility to determine physical security measures required to protect against technical penetration and eliminate technical security hazards and weaknesses.

(2) The physical and electronic examination of equipment and furnishings prior to their introduction into a sensitive facility which has previously received a TSCM Survey. This is not a requirement; however, it should be requested if there are any suspicious circumstances.

TSCM In-Conference Monitor. An electronic search to ascertain that a SECRET or above conference or meeting is not being monitored by unauthorized technical means. All locations where TSCM in-conference monitoring is to be conducted should have been the subject of a previously conducted TSCM Survey with

DoD Certified TSCM Personnel. Personnel who have successfully completed training at the approved training facility.

TSCM Pre-Construction Assistance. Support conducted during the planning stages for new construction or renovation of sensitive facilities to ensure that appropriate physical and technical security standards are met.