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

I MEFO 3850.1
G-2

22 APR 2015

I MARINE EXPEDITIONARY FORCE ORDER 3850.1

From: Commanding General, I Marine Expeditionary Force
To: Distribution List

Subj: TECHNICAL SURVEILLANCE COUNTERMEASURES (TSCM) PROGRAM

Ref: (a) Intelligence Community Directive 702
(b) Intelligence Community Directive 705
(c) SPB Issuance 1-99/2-99/3-99
(d) DoDINST 5204.05
(e) DoDINST 5240.05-M-1(S)
(f) DoDINST 5240.05-M-2(S)
(g) SECNAVINST 5510.36
(h) SECNAVINST 3850.4A
(i) MCO 5511.20
(j) Quad Service MOU USAF, USA G2X, NCIS and USMC DIRINT of 22 Oct 12
(k) SECNAVINST 5510.36 Manual ch1
(l) CMC White Letter No. 1-11
(m) SECNAVINST 5520.3B
(n) DoDINST C-5240.08

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

1. Situation. A significant technical threat is posed by the capability of all foreign intelligence or dissident domestic agents to use technical surveillance means to collect information from sensitive U.S. facilities and activities or against select targeted individuals. The threat usually takes the form of devices installed or employed at the direction of a foreign power for the specific purpose of audio, visual, or emanation collection of information from within a sensitive area. This information may be obtained by direct technical penetration, or by exploiting a technical security hazard or physical security weakness in a sensitive area. Historically, foreign intelligence services have employed 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 5511.2F.

3. Mission. This Order is intended to provide guidance for the management of the I Marine Expeditionary Force (I MEF) TSCM program, requesting criteria and procedures, conduct prior to and during a survey, and reporting

DISTRIBUTION STATEMENT B: Distribution authorized to U.S. Government agencies only. Other requests for this publication must be referred to G-2, I Marine Expeditionary Force.

requirements pertaining to TSCM services within I MEF. When properly used, TSCM services can reduce the likelihood of a technical penetration and will serve to nullify the effectiveness of technical surveillance. 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 as well as technical security hazards or vulnerabilities which may lead to a technical penetration. The I MEF TSCM team provides multiple missions to combat the threat of technical surveillance and provide commanders classified TSCM threat briefings upon request. References (a) through (k) establish policy, standards, criteria, and guidance for the I MEF TSCM program.

4. Execution

a. Commander's Intent and Concept of Operations

(1) Commander's Intent. TSCM shall be employed to the greatest extent possible, as part of comprehensive counterintelligence (CI) and security programs, in order to detect, isolate, and neutralize hostile technical surveillance operations.

(2) Concept of Operations

(a) Reference (d) designates TSCM as a CI functional service. Only TSCM-qualified practitioners may conduct TSCM activities or employ TSCM equipment, per references (d) through (i). These TSCM activities shall be conducted in accordance with the references and other technical employment guidelines as TSCM Program Manager directs. The TSCM program consists of CI technical investigations and services (such as surveys, inspections, pre-construction advice, and assistance) and technical security threat briefings. TSCM investigations and services are highly specialized CI investigations and are not to be confused with other compliance-oriented or administrative services conducted to determine a facility's implementation of various security directives.

(b) Justification and Selection of Spaces Requiring TSCM Support. Specific criteria are used to select spaces and facilities requiring TSCM support. Additionally, operational security considerations must be taken into account before, during, and after TSCM services. Exercise selectivity in identifying spaces to receive TSCM support. It is imperative that commanders employ effective physical security measures as well as implementing positive access controls in spaces where TSCM services are conducted. The following criteria determine TSCM support requirements:

1. Basic Criteria. Request TSCM support for 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. References (b) and (k) contain guidance relative to physical security matters. Reference (g) and (l) contain criteria for justification of TSCM support within the Department of the Navy and Marine Corps.

2. Conferences. Classified meetings may not be held at hotels, conference centers, or any other uncleared venue. TSCM servicing organizations may approve requests on a case-by-case basis for facilities that do not meet these requirements. For facilities that are not open to the general public and have the potential for good audio and physical security,

access control to the facility needs to be established prior to the TSCM support, throughout the conference, and continued thereafter. Failure to provide appropriate security measures once TSCM services begin until the conclusion of the conference may foster a false sense of security after TSCM services are provided. TSCM support to in-conference monitoring provides technical surveillance countermeasures for the duration of the conference only. TSCM practitioners will require access to the meeting space prior to the start of the conference.

3. New/Renovated Facilities. Facilities that process Secret information and above qualify to receive TSCM support once all construction is complete, the spaces are occupied, and security measures are in effect.

4. Pre-Construction Assistance. Any future construction concerning a facility that will 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 ensures that technical surveillance devices are not emplaced during construction and to prevent the inadvertent development of technical security hazards and vulnerabilities.

5. Automobiles, Ships, and Airplanes. TSCM support for such vehicles will not be conducted unless justified by extraordinary circumstances. Reference (g), paragraph 6a(5) pertains.

6. Equipment. Equipment such as telephones, radios, typewriters, cassette players, etc., introduced into secure areas will meet the requirements of references (b) and (k). Equipment will be inspected after it has been introduced into the facility. Such inspections will normally be conducted on the next scheduled TSCM survey unless unusual circumstances dictate otherwise.

7. Recurring Support. No facility automatically qualifies 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:

a. Evidence exists suggesting an area has been technically penetrated.

b. Extensive construction, renovation, or structural modifications required unescorted access by unclear individuals.

c. Unauthorized personnel have gained uncontrolled access to the facility.

8. 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 practitioners are trained to address unique security concerns not covered by network administrators. TSCM practitioners may investigate computers, networks, and telecommunications systems to identify technical compromise or the exploitation of digital data processed or stored on these systems. CI measures can be recommended to enhance the security of digital information from threats such as hacking, phreaking, and foreign intelligence exploitation. TSCM personnel may inspect

both logical and physical components of computers, computer networks, and telephony systems to identify technical compromise or surreptitious extraction of information from the area.

9. Commanding General (CG) Directed Areas. In the interest of protecting sensitive/classified information, facilities may be selected by I MEF CG for a TSCM survey. In such cases, the selected facility will be notified prior to the survey in order to coordinate the required command cooperation to complete the survey.

10. 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. Subordinate Element Missions

(1) Assistant Chief of Staff (AC/S), G-2/Staff CI Officer, I MEF. Exercise overall staff cognizance for the TSCM program within I MEF and validate all TSCM requests.

(2) Senior Marine Corps CI Officer/Enlisted assigned as CI Human Intelligence (CI/HUMINT) Officer (CIHO), I MEF

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

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

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

(3) Commanding Officer, 1st Intelligence Battalion

(a) Upon direction of the I MEF CG, provide TSCM support in accordance with criteria established by this Order, references, and applicable guidance.

(b) Ensure that administrative, logistical, and communications support is provided to the TSCM team to support I MEF requirements.

(c) Budget for annual TSCM refresher training.

(d) Staff trained TSCM practitioners at a level commensurate with annual tasking, in addition to reasonable contingency surge requirements.

(4) CI/HUMINT Company Commander

(a) Provide trained and qualified TSCM practitioners for TSCM support upon direction.

(b) Budget for TSCM expendable supplies.

(5) TSCM Officer in Charge

(a) Provide TSCM threat data to the Commanding Officer I MEF via the CIHO and AC/S G-2.

(b) Provide copies of TSCM reporting to the CIHO for the purpose of archiving and maintaining all records relating to TSCM.

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

(6) TSCM Team Leader

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

(b) Conduct liaison with USMC TSCM Program Manager.

c. Coordinating Instructions

(1) Request Procedures. Due to manpower constraints, all routine requests for TSCM service may not be fulfilled immediately and will be handled on a prioritized basis each calendar year. A request for TSCM support shall be valid for a period of two years. Due to the sensitive nature of TSCM support, correspondence and knowledge of TSCM support shall be kept to an absolute minimum. Information pertaining to pending, planned, or ongoing TSCM support must not be discussed in the area in which the TSCM activities are taking or will take place do not discuss TSCM matters over unsecure telephones or telephones located in facilities/rooms pending or scheduled for TSCM support in accordance with paragraph 6(c) of reference (g) and reference (n). Should a command discover a clandestine surveillance device, follow the guidance in enclosure (1). To request TSCM support, follow the guidance in enclosure (2).

(a) Submit all requests for I MEF TSCM support to CG, I MEF, (Attn: AC/S G-2) via G-2/Staff CI Human Intelligence Officer (CIHO) per enclosure (2) for validation.

(b) Upon validation of requirements by the AC/S G-2, the Commanding Officer of 1st Intelligence Battalion will be tasked with providing TSCM operations. Due to the sensitive nature of TSCM requests, specific details pertaining to the requests will be sent only to the TSCM team.

(c) Upon receipt of validated tasking, TSCM Team Leader will coordinate with the CIHO to prioritize and schedule TSCM support.

(d) Upon approval and direction by the CG I MEF, 1st Intelligence Battalion will provide TSCM services and support to non-Fleet Marine Force (FMF) commands when requested by the USMC TSCM Program Manager.

(e) Support to other services and support received by I MEF from other TSCM units will be conducted in accordance with reference (j).

(2) Support Priority. Upon receipt of validated tasking for TSCM support, I MEF TSCM Team will schedule support. First priority will be to

FMF commands, followed by Marine Corps non-FMF commands, and then commands of other services.

(3) Operational Security (OPSEC). TSCM services are specialized CI 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. For this purpose assume, until the survey indicates otherwise, that an eavesdropping device is actually in place. 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 switched off 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 practitioners will immediately terminate the provided support and report the circumstances which compromised the TSCM support CG I MEF, via the I MEF G-2. Likewise, 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 within 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 (k) and paragraph 6f of reference (m).

(4) Reporting. 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 Manager. Reports shall be forwarded to the requester no more than 30 working days after the completion of services. 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. Technical Penetration and Technical Hazard reporting will be conducted in accordance with reference (c). All requests, validations and reporting will be forwarded to Marine Corps TSCM Program Manager for archiving. Commands that are the subject of TSCM services with findings will respond to TSCM reports within 90 business days to address corrective actions, acceptance of risk, or refutation of findings.

5. Administration and Logistics

a. Administration. The nature of TSCM, as a specialized CI 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. Per reference (d), only Department of Defense (DoD) certified TSCM practitioners will conduct TSCM services. I MEF TSCM practitioners shall receive, at least annually, refresher or other specialized training to remain proficient and knowledgeable concerning technical penetration and/or detection techniques, in accordance with references (d) through (i).

b. Logistics. 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 returned to the TSCM Program Manager.

TSCM equipment should be shipped via Defense Courier Service or other secure means.

6. Command and Signal

a. Command

(1) The CG, I MEF, through the AC/S G-2, has operational control of the I MEF TSCM Program. This Order is applicable to all commands, organizations, units and activities under the cognizance of I MEF.

(2) The TSCM team has direct liaison authority with Marine Corps TSCM Program Manager on TSCM equipment and technical matters.

b. Signal. This Order is effective the date signed.

M. G. GOUGH
Chief of Staff

Distribution: I/II

Copy to: CO, I MHG
CO, 1st Intel Bn

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. 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 Team for action. By December 1st of each year, Major Subordinate Commands and Elements 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. Commands should correct weaknesses identified during previous TSCM services.

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. Non-local requests must be funded by the requesting unit; therefore, non-local requests must include appropriation data for travel claim purposes. I MEF TSCM personnel will make every effort to procure Government/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

TSCM: Those techniques conducted to detect, neutralize, and exploit technical surveillance technologies and hazards which facilitate the unlawful access to, or removal of, DoD information. An electronic and physical examination of the total environment (including telecommunication networks, infrastructure, and components) in and around a facility, vehicle, or geographic location, to identify the presence of technical surveillance and conditions that could facilitate technical surveillance.

Item of Security Interest: An unexploited condition that, by itself, is not a technical or physical vulnerability but can degrade or contributes to the degradation of the overall security posture of the area to the point where the condition could facilitate a technical or physical vulnerability.

Physical Vulnerability: An unexploited condition occurring in the physical infrastructure of a facility that could facilitate the unauthorized removal of information bearing energy through either mechanical or electrical means.

Technical Hazard: An unexploited condition wherein information-bearing energy might be intercepted and compromised.

Technical Penetration: The use of technological means to conduct an intentional, unauthorized interception of information-bearing energy.

TSCM Survey: This is an all-encompassing investigation. This investigation is a complete electronic, physical, and visual examination to detect clandestine surveillance systems. A by-product of this investigation is the identification of physical and technical security weaknesses that could be exploited by enemy intelligence forces.

TSCM Inspection: Normally, once a TSCM survey has been conducted, it will not be repeated. If TSCM practitioners note several technical and physical weaknesses during the survey, they may request and schedule an inspection at a later date. In addition, they will schedule an inspection if there has been an increased threat posed to the facility or if there is some indication that a technical penetration has occurred in the area. No facility, however, will qualify automatically for recurrent TSCM support.

TSCM Pre-construction Assistance: As with other technical areas, it is much less expensive and more effective to build in good security from the initial stages of a new project. Thus, pre-construction assistance is designed to help security and construction personnel with the specific requirements needed to ensure that a building or room will be secure and built to standards. This saves money by precluding costly changes later on.

TSCM Practitioner: DoD CI credentialed personnel who have completed the Interagency Training Center (ITC) Fundamentals Course and have been certified to conduct the full range of TSCM activities by the head of the hiring component. Marine TSCM practitioners must be Marines credentialed as CI agents holding the PMOS 0211 and NMOS 0212 (TSCM Specialist), or Warrant Officers holding PMOS 0210 who have completed both the U.S. Army TSCM Course and the ITC TSCM Fundamentals Course.