SECRET

DEPARTMENT OF THE NAVY
HEADQUARTERS UNITED STATES MARINE CORPS
WASHINGTON, D. C. 20380

MCO 005511.11A
AO2A-BRG-req
15 Jul 1971

SECRET NO FOREIGN DISSEM

MARINE CORPS ORDER 005511.11A

From: Commandant of the Marine Corps
To: Distribution List

Subj: Technical Surveillance Countermeasures (U)

Ref: (a) OPNAVINST 5510.1C
(b) OPNAVINST 5510.45B
(c) SECNAVINST 5430.13B
(d) KAG-1D/TSEC
(e) OPNAVINST 005500.46A

Encl: (1) Locator Sheet

1. (C) Purpose. To reiterate the necessity for protection of classified information against technical penetration, provide information regarding technical surveillance countermeasures (TSCM) for inclusion within the command security programs, and furnish information as to the availability of TSCM support to Marine Corps commands.

2. (U) Cancellation. MCO 005511.11.

3. (S) Background. Technological advances and the application of new techniques and concepts have increased the threat of technical penetration by hostile intelligence elements. During the past 5 years hostile penetrations utilizing clandestine listening devices have been mainly directed at political targets. The discovery of these penetrations, however, has revealed a continued extensive hostile capability which can also be directed at U. S. military installations. Furthermore, the availability of electronic components and subassemblies on the commercial market has increased the threat of low-level technical penetration. The threat to military installations is considered less than that to certain other Government installations; however, the extensive hostile capability dictates that positive technical surveillance countermeasures are applied for the protection of highly classified or sensitive information.

UNCLASSIFIED

4. (S) Information. The sophistication of technical penetration techniques may range from simple wired microphones to direct transmission optical links utilizing light rays which are beyond the wave length visible to the human eye. The

Declassified / Downgrade to
Auth: EO 12958 2 Sept 98
DOWNGRADING AT 12 YEAR INTERVALS;
NOT AUTOMATICALLY DECLASSIFIED.
DOD DIR 5200.10
Date: Unit: NCIS 22

SECRET
PCN 102 085000 00

DECLASSIFIED
Authority NND 73643

most common techniques which have been employed to date include the use of wire microphones, radio frequency transmitters, and exploitation of existing telephones or intercommunications systems. The single most effective countermeasure against technical penetration is a continuous and vigorous physical security program including strict access control. The following specific countermeasures concepts are utilized in maintaining a proper security posture against the threat of technical penetration and surveillance.

a. (S) Isolation. Isolation is accomplished by ensuring that highly classified or sensitive information is discussed only in areas which are afforded complete perimeter and access control. In addition to proper physical security measures, acoustic control (soundproofing) and electromagnetic control (RF shielding) may also be necessary depending on the area. Intercommunication systems and telephones should be removed from sensitive spaces such as conference and briefing rooms wherever practical. When removal of telephones is impractical, they should be equipped with a secondary disconnect device, such as a jack and plug, in order to physically disconnect the instrument from the line when not in use. Access to these areas must be stringently controlled. Uncleared personnel and foreign nationals must be excluded or escorted and closely supervised at all times. Escorts must be appropriately cleared U. S. personnel aware of the threat of technical penetration. It must be impressed on personnel concerned with the security of sensitive areas, that an RF transmitter can be installed in as little as 15 seconds once access is gained to an area. Additional guidance and information concerning command responsibility for physical security are contained in references (a) and (b).

b. (S) Nullification. Nullification is a method of masking or jamming classified conversation by the use of various sound sources which will render the intercepted information unintelligible. Appropriate sound sources include radio and television broadcasts or prerecorded multiple conversation. Nullification is not effective over a long period of time and should only be used as an expedient when circumstances preclude establishing appropriate isolation.

c. (S) Detection

UNCLASSIFIED

(1) (S) To augment isolation and nullification a program of detection directed toward locating and neutralizing clandestine listening devices should be instituted. Advances in

technology and new techniques normally require highly skilled personnel using specialized countermeasures equipment and techniques to locate clandestine listening devices. Techniques now exist, for example, wherein a telephone may be used as a listening device without modification to the instrument and without the telephone being in use.

(2) (C) The advancement in technical penetration capabilities has necessitated corresponding advancement in countermeasures equipment and techniques which in turn has dictated consolidation of TSCM assets due to rising costs and greater training requirements.

5. (C) Responsibility

a. (C) Reference (c) established the Naval Investigative Service (NIS) responsibility for providing specialized TSCM support within the Department of the Navy. TSCM support to CONUS and the Western Hemisphere is provided from NIS Headquarters, Alexandria, Virginia. NIS Office Europe, London, England, provides support for Europe and Africa; and NIS Pacific, Honolulu, Hawaii, provides support to the Pacific area.

b. (C) Selected Marine counterintelligence teams also maintain a limited tactical TSCM support capability. While these teams may be utilized for advice to all commanders concerning their TSCM programs, this detection support capability should be limited, except for unusual circumstances, to tactical units of the Fleet Marine Forces.

6. (C) Inspections and Surveys

a. (C) TSCM support is provided by TSCM inspections and surveys which differ only in the degree of support provided. Discussions concerning such support should not take place in the area which is to be inspected or surveyed. In addition, all requests and reports concerning TSCM support should be classified at least confidential.

b. (C) Sensitive areas requiring TSCM inspections or surveys are normally limited to fixed secure communication facilities as required by reference (d), those areas where highly classified information is discussed on a continuous basis, and those areas where special intelligence or extremely sensitive programs are normally discussed. Areas which are determined to require TSCM inspections or surveys must also

contain appropriate physical security and access control systems to preclude unauthorized access. Sensitive areas should be inspected no less than annually and when circumstances indicate that a possibility of technical penetration exists, such as new construction, renovation, repairs, or unauthorized access.

c. (C) Whenever possible, conferences and meetings concerning highly classified or sensitive matters should be held in secure areas which have previously received TSCM inspections or surveys.

7. (S) Action

a. (C) Commanders will ensure that appropriate technical surveillance countermeasures are included in their overall security programs. Those commands maintaining sensitive areas and requiring NIS TSCM support should submit requests to the appropriate NIS headquarters contained in paragraph 5a, above. Further instructions for requesting TSCM support are contained in reference (e).

b. (S) In the event a technical penetration is discovered, classified conversation in the area should be sanitized to a minimum level and terminated as soon as feasible. Normal routine should be maintained in the area to the extent possible and no verbal reference should be made concerning the discovery. The Commandant of the Marine Corps (Code AO2), Commander, Naval Intelligence Command, Director, Naval Investigative Service, and appropriate commanders will be immediately notified of the discovery. Detailed action to be taken in the event of a technical penetration discovery is contained in reference (e). Information concerning discoveries will be classified secret.

8. (U) Reserve Applicability. This Order is applicable to the Marine Corps Reserve.

J. R. CHAISSON
Chief of Staff

DISTRIBUTION: 5/10 plus 7000032, 046, 062, 078(2)

Copy to: Naval Intelligence Command
Naval Investigative Service

UNCLASSIFIED

Declassified / Downgrade to.....
Auth: EO 12958
Date: 21 SEP 98 Unit: NCISHQ

SECRET

LOCATOR SHEET

Subj: Technical Surveillance Countermeasures

Location: _____

(Indicate the location(s) of the copy(ies) of this publication.)