UNITED STATES MARINE CORPS
MARINE CORPS COMBAT DEVELOPMENT COMMAND
QUANTICO, VIRGINIA 22134-5001

MCCDCO 3070.1B
C03/k
23 Jun 93

MARINE CORPS COMBAT DEVELOPMENT COMMAND ORDER 3070.1B

From: Commanding General
To: Distribution List

Subj: COMMAND OPERATIONS SECURITY (OPSEC) AND SIGNAL SECURITY (SIGSEC) PROGRAM

Ref: (a) FMFM 3-1
(b) JCS Pub 1
(c) OPNAVINST 3070.1A
(d) MCCDCO P5400.1A
(e) OPNAVINST 5510.1H
(f) MCCDCO 3850.2A
(g) SECNAVINST 5500.31A

Encl: (1) OPSEC References and Guidance

1. Purpose. To establish the OPSEC/SIGSEC Council and promulgate guidance and instructions for implementing the Command OPSEC and SIGSEC Program.

2. Cancellation. MCCDCO 3070.1A.

3. Summary of Revision. This revision reflects changes in organization and organizational titles of the Marine Corps Combat Development Command (MCCDC) and reassigns responsibilities and tasks according to the revised organization.

4. Background

a. OPSEC is the discipline of controlling indicators (information or overt practices) through which an adversary can deduce capabilities and intentions of forthcoming operations and activities. Proper OPSEC requires the identification of indicators about friendly capabilities and intentions associated with military operations and other activities and then protecting or controlling those indicators that are susceptible to hostile exploitation. The objective of OPSEC is to prevent an adversary from collecting enough information to accurately predict friendly actions. Historically, OPSEC evolved as an entity after security surveys showed that stereotyped U.S. operational procedures and predictable patterns, as well as open sources of information and poor communications security, can provide an alarming amount of intelligence to an adversary.

b. OPSEC as a formal concept was originated in the late 1960's. Other concepts and security disciplines encompassing

aspects of OPSEC were originated earlier than or subsequent to its development. Such was the case of SIGSEC. OPSEC is not specifically concerned with the management of other security programs nor is it necessarily an "umbrella" for all other security disciplines; its interest is oriented more towards those instances in which evaluations indicate weaknesses that result in indicators and open sources of information or exploitation of operational procedures or security practices. The principal characteristics that distinguish OPSEC from other security programs are the broad scope and concern with all exploitable information; a systematic approach to determining essential secrecy, identifying sources and vulnerabilities, and determining OPSEC measures through OPSEC planning; a case-by-case focus on adversary threats; and an emphasis on action and follow-up to preserve essential secrecy. The enclosure provides a listing of OPSEC references for guidance and general information.

5. Information

a. Reference (a) specifies that staff cognizance for planning and execution of OPSEC and SIGSEC is a function of the Operations Department/G-3 staff. In consonance with reference (a), the Director, Operations Division, is responsible for the planning and direction of the OPSEC/SIGSEC Program at MCCDC.

b. The following specific definitions, as contained in reference (b), are used to clarify terminology and provide specificity and consistency within the Command OPSEC/SIGSEC Program:

(1) OPSEC. The process of denying adversaries or potential adversaries information about friendly operations, as well as friendly capabilities and intentions by identifying, controlling and protecting information and other indicators associated with planning and execution of military operations and other activities.

(2) SIGSEC. A generic term that includes both communications security (COMSEC) and electronic security.

(3) COMSEC. The protection resulting from all measures to deny unauthorized persons information of value which might be derived from the possession and study of telecommunications, or to mislead unauthorized persons in their interpretation of the results of such possession and study. COMSEC includes cryptosecurity, transmission security, emission security and physical security of communications security material and information.

(4) Electronic Security. The protection resulting from all measures designed to deny unauthorized persons information of value that might be derived from their interception and study of noncommunications electromagnetic radiation.

c. The mission objective of the OPSEC/SIGSEC Program at MCCDC is to effectively anticipate security requirements, and to properly plan for and execute effective measures designed to detect, neutralize, or destroy the effectiveness of actual or potential hostile foreign or industrial intelligence collection, sabotage, or subversive activity, and to provide necessary protection for information, personnel, equipment, and facilities against compromise, sabotage, and terrorism. OPSEC/SIGSEC is properly an operational function and responsibility of every level in the chain of command to ensure the general security of the Command. Both active and passive OPSEC/SIGSEC measures, including organic and external assets, will be used at this Command to fulfill OPSEC/SIGSEC requirements.

d. The OPSEC/SIGSEC Council is a means by which the Commanding General gains full Command involvement in the design and implementation of the OPSEC/SIGSEC Program. The membership is assigned as follows, and will meet at the call of the Director, Operations Division.

Director, Operations Division (Chairman)
Command Adjutant
Provost Marshal
Head Communications Branch, Communications Electronics Division, Marine Corps Computer and Telecommunications Activity
Staff Judge Advocate
Public Affairs Officer
Representative, Marine Corps Intelligence Activity
Naval Investigation Service Resident Agent

6. Action

a. As prescribed in reference (c), all activity heads will evaluate assigned functions from an OPSEC perspective and specifically:

(1) Identify those assigned functions or events of potential interest to adversaries under various circumstances.

(2) Determine indicators about Command intentions, capabilities and activities that might be conveyed by executing assigned functions.

(3) Prepare Command OPSEC plans as required to control or protect indicators.

(4) Train Command personnel so they are capable of executing appropriate OPSEC measures appropriate to their duties.

b. OPSEC/SIGSEC Council. When convened among other OPSEC duties and responsibilities, the council will perform the following specific functions:

(1) Evaluate the effectiveness of current MCCDC security.

(2) Evaluate the results of security related inspections, surveys, and exercises and recommend corrective actions.

(3) Review installation entry and visitor control procedures.

(4) Recommend priorities for the commitment of MCCDC security resources to the Commanding General.

c. Director, Operations Division

(1) Develop, review, and modify, as may be required, contingency plans and orders for OPSEC and SIGSEC requirements for the Command.

(2) Chair the MCCDC OPSEC/SIGSEC Council and coordinate the Command OPSEC/SIGSEC Program to include overall physical security and counterterrorism planning.

d. Head, Communications Branch, Communication Electronics Division, Marine Corps Computer and Telecommunications Activity

(1) Act as member of the OPSEC/SIGSEC Council.

(2) In addition to the functions detailed in reference (d), provide appropriate COMSEC for communications electronics systems. This includes security for telephones and telefax systems as may be required.

(3) Be prepared to provide for technical assistance and appropriate management initiatives in conjunction with possible emerging requirements relative to installation of secure voice, secure telefax, World Wide Military Command and Control System (WWMCCS) terminals and other electronic systems as those requirements become known.

(4) In addition to support contained in reference (c), assume responsibility of, and provide support for evaluation and control, as may be required, relative to electromagnetic emissions from office machines and computers/printers as well as methods for security of information storage systems. (Tempest requirement coordination and site surveys for equipment placement.) Reference (e) applies for ADP security matters.

e. Security Manager/Provost Marshal

(1) Act as member of the OPSEC/SIGSEC Council.

(2) Provide military police, criminal investigative support to the Command to include appropriate crime prevention measures. As Security Manager, ensure physical security activity, and supervisory

actions for protection of classified material per references (d) through (f). Security Manager support will include measures contained in reference (e).

(a) The following areas and spaces will be physically inspected every 90 days for signs of hostile special intelligence gathering. A schedule and log of these activities will be prepared and maintained by separate staff action to be supervised by the Security Manager. Inspections may be made more frequently upon request of the occupants and/or appropriate authority should area security be questioned as a result of uncleared maintenance personnel or contract worker access; known or suspected evidence of tampering; or a known requirement to discuss classified material during conferences or meetings.

1 Commanding General, MCCDC, Office Suite, Lejeune Hall.

2 Chief of Staff, MCCDC, Office Suite, Lejeune Hall.

3 Commanding General's Conference Room (room 218), Lejeune Hall.

4 Quarters 1, MCCDC (as requested).

5 President, Marine Corps University, Office Suite, Butler Hall.

6 President, Marine Corps University, Conference Room, Butler Hall.

7 Special Compartmented Information Facility (SCIF), Hochmuth Hall (Physical inspections/technical surveillance counter-measures (TSCM) coordinated by Marine Corps Intelligence Activity personnel).

8 MCCDC Communication Center, Rooms 008 and 016, Lejeune Hall.

9 MCCDC WWMCCS, Room 217, Lejeune Hall.

(b) Additional technical inspections and evaluations, as well as physical inspections may be conducted annually, assets permitting, for these and other spaces to be designated by the Director, Operations Division. Requests for technical inspections will be classified SECRET when areas and times are identified. Under no circumstances will a technical inspection be discussed verbally within the area of concern, nor on the telephone. Reference (g) applies.

1 Schedules and procedures for unannounced after hours security inspections by Security Manager personnel will be conducted regularly as directed by the Director, Operations Division. The Director, Operations Division will coordinate such inspections with the Security Manager. Reference (f) applies.

2 Special technical surveillance may be conducted per reference (e) at the specific direction of the Commanding General, when duly authorized by proper authority.

(c) Courtesy security inspections/appraisals/evaluations will be conducted when requested to the extent considered reasonable and practical by the Security Manager. When conducted, this will normally include:

1 Inspections of furniture, fixtures, and decorations for concealed electronic or photographic devices.

2 Evidence of tampering to any electronic devices, instruments, fixtures, outlets or appliances.

3 Inspections of sensitive areas where maintenance or contracted work has been recently performed.

f. Staff Judge Advocate. Act as member of the OPSEC/SIGSEC Council.

g. Command Adjutant

(1) Act as a member of the OPSEC/SIGSEC Council.

(2) Manage internal security for the MCCDC Headquarters (Building 3250), to include access to the Headquarters Building, monitoring visitors and construction/repair work in the Headquarters Building, and security for office spaces in the Headquarters Building.

h. Public Affairs Officer

(1) Act as a member of the OPSEC/SIGSEC Council.

(2) Ensure internal and external information sources are per appropriate security review procedures.

i. Marine Corps Intelligence Activity Detachment (Quantico)

(1) Provide a representative to the OPSEC/SIGSEC Council.

(2) Provide Special Security Officer services and advice to the Commanding General, MCCDC as may be required.

(3) Be prepared to coordinate secure conference room space within the SCIF to the Command for meetings at special levels of classification suitable for properly cleared military and civilian personnel, to include very important persons and distinguished visitors.

(4) As required, provide assistance to the Director, Operations Division regarding those broad planning responsibilities for intelligence and counterintelligence normally under the staff cognizance of an Assistant Chief of Staff, G-2. Tasking for intelligence and counterintelligence assets will remain via the currently established chain of command.

j. Naval Investigative Service Resident Agent

(1) Act as a member of the OPSEC/SIGSEC Council.

(2) Provide multi-discipline counterintelligence in conjunction with OPSEC planning.

(3) Provide indications of foreign intelligence interest in systems acquisition programs and systems in service use.

(4) On request, provide counterintelligence and physical security personnel to conduct formal OPSEC surveys.

(5) On request, coordinate OPSEC/SIGSEC training.

(6) Coordinate TSCM support.

M. R. STEELE
Commanding General
Marine Corps Base

DISTRIBUTION: A plus 6 (10)

OPSEC REFERENCES AND GUIDANCE

1. DoD Directive 5205.2, 7 Jul 83, DoD Operations Security Program

2. JCS Pub 18, 15 Dec 82, Policy, Concepts and Standards for Operations Security

3. JCS OPSEC Survey Planning Guide, J3M-947-83, 15 Jun 83

4. Joint Operation Planning System, Vol 1, JCS Pub 5-02.1, 6 Jul 88 Format for OPSEC Annex L (Chapter 6)

5. Joint Operation Planning System, Vol 2, JCS Pub 5-02.2, 30 Mar 90, Planning Guidance -- Operations Security Annex (Annex L)

6. SECNAVINST 3070.1, 9 Aug 84, Operations Security

7. OPNAVINST 3070.1A, 24 Jun 85, Operations Security

8. FM 90-2, Battlefield Deception