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

IN REPLY REFER TO:
I MEFO 5240.1
G-2
MAY 8 2017

I MARINE EXPEDITIONARY FORCE ORDER 5240.1

From: Commanding General
To: Distribution List

Subj: COUNTERINTELLIGENCE AWARENESS AND REPORTING

Ref: (a) DODD 5240.06
(b) DODI 5240.04
(c) DODD 2000.12
(d) DODD O-5240.02
(e) SECNAVINST 3850.2D
(f) MCBUL 1500

Encl: (1) Reportable Indicators

1. Situation. Reference (a) is the Department of Defense (DOD) mandate for Counterintelligence Awareness and Reporting (CIAR) training. Reference (b) requires significant counterintelligence activities and instances of espionage to be reported expeditiously. Reference (c) requires the sharing of Antiterrorism/Force Protection (ATFP) related counterintelligence (CI) information. Reference (d) is the DOD policy for CI. Reference (e) directs USMC DIRINT to develop and implement CI awareness briefings, threat mitigation activities, and reporting procedures for the USMC. Reference (f) identifies CIAR training as an annual training requirement. This Order outlines regulations for the implementation of the CIAR program within I Marine Expeditionary Force (I MEF), and establishes policies and procedures for the conduct of the program. This program will be coordinated with the Director Naval Criminal Investigative Service.

2. Mission. To establish a CIAR program within I MEF that facilitates I MEF personnel recognizing threats and reporting threat information associated with terrorism, espionage, sabotage, subversion, and insider threats. The CIAR program provides education to I MEF personnel on these threats, and establishes reporting channels to aid in identifying information associated with threat Indications and Warnings (I&W).

3. Execution

a. Commander's Intent and Concept of Operations

(1) Commander's Intent

(a) Per references (a), (b), and (e), all I MEF personnel are required to report information or circumstances that could pose a threat to

the security of DOD personnel, resources, or classified or controlled defense information.

(b) I MEF personnel shall report contacts, activities, indicators, and behaviors associated with potential FIE threats to I MEF CI Agents as directed within the CIAR brief.

(c) When it is not feasible to report incidents to CI personnel, I MEF personnel shall report to security officers, supervisors, and commanders.

(d) Security officers, supervisors, and commanders shall also follow these reporting requirements.

(2) Concept of Operations. Per reference (a) and (f), all I MEF personnel must receive CIAR training, as outlined in this Order, each calendar year.

b. Training Requirements

(1) CIAR training shall include instruction on:

(a) The threat from Foreign Intelligence Entities (FIE).

(b) The methods of FIE.

(c) FIE use of the internet and other means of communication, including social networking services.

(d) The CI insider threat.

(e) Reporting responsibilities and requirements.

(2) All I MEF personnel shall receive CIAR training within 90 days of initial assignment or employment, and each calendar year thereafter.

(3) I MEF CI Agents shall provide training in a classroom environment, tailored to the individual or unit mission, functions, activities, and location.

(4) Records of CIAR training will be kept at the unit level and include the following:

(a) Attendees.

(b) Trainer and his or her organization.

(c) Date(s) of training.

(d) Subject of training and a summary of the training content.

c. Tasks

(1) I MEF Assistant Chief of Staff G-2

(a) Coordinate requests for CIAR training with I MEF Major Subordinate Command (MSC) CI/HUMINT Representative and Major Subordinate Elements (MSEs) S-2 Officers.

(b) Maintain current CIAR training curriculum for CI Agents to conduct training with I MEF commands.

(c) Maintain training records.

(2) Major Subordinate Commands and Elements

(a) Ensure all Marines receive CIAR training per this Order.

(b) Maintain training records for personnel who have received CIAR training.

(3) Commanding Officer, I MEF Headquarters Group

(a) Provide counterintelligence agents to support CIAR training upon direction from the I MEF G2X.

(b) Submit copies of training records to I MEF G2X.

d. Coordinating Instructions. Request procedures and points of contact from the following:

(1) I MEF Headquarters Group and Major Subordinate Elements requests for training should be coordinated through I MEF G2X at (760) 763-4614 or IMEFCEG-2X@usmc.mil.

(2) MSC requests for training should be coordinated through the MSC G2 CI Representative.

(a) 1st Marine Division. (760) 725-9835.

(b) 1st Marine Logistics Group. (760) 763-9165.

(c) 3rd Marine Aviation Wing. (858) 577-7431.

4. Administration and Logistics

a. Records of CIAR training will be kept for a period of 5 years.

b. Reference (f) establishes CIAR training as a Calendar Year requirement.

5. Command and Signal

a. Command. This Order applies to active duty and reserve Marines and Sailors, DOD civilians, and contractors assigned to I MEF.

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

LEWIS A. CRAPAROTTA

DISTRIBUTION: I/II

REPORTABLE INDICATORS

Foreign Intelligence Contacts, Activities, Indicators, and Behaviors

1. When not related to official duties, contact with anyone known or believed to have information of planned, attempted, actual, or suspected espionage, sabotage, subversion, or other intelligence activities against DoD facilities, organizations, personnel, or information systems. This includes contact through SNS that is not related to official duties.

2. Contact with an individual who is known or suspected of being associated with a foreign intelligence or security organization.

3. Visits to foreign diplomatic facilities that are unexplained or inconsistent with an individual's official duties.

4. Acquiring, or permitting others to acquire, unauthorized access to classified or sensitive information systems.

5. Attempts to obtain classified or sensitive information by an individual not authorized to receive such information.

6. Persons attempting to obtain access to sensitive information inconsistent with their duty requirements.

7. Attempting to expand access to classified information by volunteering for assignments or duties beyond the normal scope of responsibilities.

8. Discovery of suspected listening or surveillance devices in classified or secure areas.

9. Unauthorized possession or operation of cameras, recording devices, computers, and communication devices where classified information is handled or stored.

10. Discussions of classified information over a non-secure communication device. Reading or discussing classified or sensitive information in a location where such activity is not permitted.

11. Transmitting or transporting classified information by unsecured or unauthorized means.

12. Removing or sending classified or sensitive material out of secured areas without proper authorization.

13. Unauthorized storage of classified material, regardless of medium or location, to include unauthorized storage of classified material at home.

14. Unauthorized copying, printing, faxing, e-mailing, or transmitting classified material.

15. Improperly removing classification markings from documents or improperly changing classification markings on documents.

16. Unwarranted work outside of normal duty hours.

17. Attempts to entice co-workers into criminal situations that could lead to blackmail or extortion.

18. Attempts to entice DoD personnel or contractors into situations that could place them in a compromising position.

19. Attempts to place DoD personnel or contractors under obligation through special treatment, favors, gifts, or money.

20. Requests for witness signatures certifying the destruction of classified information when the witness did not observe the destruction.

21. Requests for DoD information that make an individual suspicious, to include suspicious or questionable requests over the internet or SNS.

22. Trips to foreign countries that are:

a. Short trips inconsistent with logical vacation travel or not part of official duties.

b. Trips inconsistent with an individual's financial ability and official duties.

23. Unexplained or undue affluence.

a. Expensive purchases an individual's income does not logically support.

b. Attempts to explain wealth by reference to an inheritance, luck in gambling, or a successful business venture.

c. Sudden reversal of a bad financial situation or repayment of large debts.

International Terrorism Contacts, Activities, Indicators, and Behaviors

1. Advocating violence, the threat of violence, or the use of force to achieve goals on behalf of a known or suspected international terrorist organization.

2. Advocating support for a known or suspected international terrorist organizations or objectives.

3. Providing financial or other material support to a known or suspected international terrorist organization or to someone suspected of being an international terrorist.

4. Procuring supplies and equipment, to include purchasing bomb making materials or obtaining information about the construction of explosives, on behalf of a known or suspected international terrorist organization.

5. Contact, association, or connections to known or suspected international terrorists, including online, e-mail, and social networking contacts.

6. Expressing an obligation to engage in violence in support of known or suspected international terrorism or inciting others to do the same.

7. Any attempt to recruit personnel on behalf of a known or suspected international terrorist organization or for terrorist activities.

8. Collecting intelligence, including information regarding installation security, on behalf of a known or suspected international terrorist organization.

9. Familial ties, or other close associations, to known or suspected international terrorists or terrorist supporters.

10. Repeated browsing or visiting known or suspected international terrorist websites that promote or advocate violence directed against the United States or U.S. forces, or that promote international terrorism or terrorist themes, without official sanction in the performance of duty.

FIE-Associated Cyberspace Contacts, Activities, Indicators, and Behaviors

1. Actual or attempted unauthorized access into U.S. automated information systems and unauthorized transmissions of classified or controlled unclassified information.

2. Password cracking, key logging, encryption, steganography, privilege escalation, and account masquerading.

3. Network spillage incidents or information compromise.

4. Use of DoD account credentials by unauthorized parties.

5. Tampering with or introducing unauthorized elements into information systems.

6. Unauthorized downloads or uploads of sensitive data.

7. Unauthorized use of Universal Serial Bus, removable media, or other transfer devices.

8. Downloading or installing non-approved computer applications.

9. Unauthorized network access.

10. Unauthorized e-mail traffic to foreign destinations.

11. Denial of service attacks or suspicious network communications failures.

12. Excessive and abnormal intranet browsing, beyond the individual's duties and responsibilities, of internal file servers or other networked system contents.

13. Any credible anomaly, finding, observation, or indicator associated with other activity or behavior that may also be an indicator of terrorism or espionage.

14. Data exfiltrated to unauthorized domains.

15. Unexplained storage of encrypted data.

16. Unexplained user accounts.

17. Hacking or cracking activities.

18. Social engineering, electronic elicitation, e-mail spoofing or spear phishing.

19. Malicious codes or blended threats such as viruses, worms, trojans, logic bombs, malware, spyware, or browser hijackers, especially those used for clandestine data exfiltration.