UNITED STATES MARINE CORPS
MARINE AVIATION DETACHMENT NAS PATUXENT RIVER
22401 CEDAR POINT ROAD, BUILDING 102
NAVAL AIR STATION
PATUXENT RIVER, MARYLAND 20670-1188

DetO 3070.1
CO
8 Dec 21

DETACHMENT ORDER 3070.1

From: Commanding Officer, Marine Aviation Detachment NAS Patuxent River
To: Distribution List

Subj: OPERATIONS SECURITY

Ref: (a) MCO 3070.2A
(b) DoD Directive 5205.02E
(c) DoD Manual 5205.02M
(d) SECNAVINST 3070.2A
(e) NASPAXRIVINST 3432.1C
(f) SECNAVINST 5720.47B

Encl: (1) Critical Information List
(2) Critical Indicators List
(3) OPSEC Countermeasures Examples
(4) Family OPSEC Brochure

1. Situation

a. References (a) through (d) guide the development of an operations security (OPSEC) program. Reference (e) provides specific OPSEC program guidance to the Marine Aviation Detachment (MAD) Naval Air Station (NAS) Patuxent River. Reference (f) provides policy guidance on the content of publicly accessible websites.

b. OPSEC is a process of identifying critical information and subsequently analyzing friendly actions attendant to military operations and other activities to:

(1) Identify those actions that can be observed by adversary intelligence systems.

(2) Determine what OPSEC indicator hostile intelligence systems might obtain that could be interpreted or pieced together to derive critical information in time to be useful to adversaries.

(3) Select and execute OPSEC measures that eliminate or reduce to an acceptable level, the vulnerabilities of friendly actions to adversary exploitation.

2. Mission. To ensure all personnel are in compliance with the references, and to establish policy and procedural guidance concerning the MAD OPSEC Program.

3. Execution

a. Commander's Intent. Incorporate the OPSEC planning process into operations, exercises, activities, system development, and test and evaluation in garrison and deployed environments as directed in reference (a).

b. Concept of Operations

(1) Reference (a) directs Marine Corps units to establish and maintain an OPSEC program that promotes an understanding of OPSEC among all personnel. The order provides policy, responsibilities and procedures for OPSEC within the MAD.

(2) OPSEC shall be integrated into all day-to-day activities and operations that prepare, sustain or deploy MAD Marines. The responsibility for OPSEC rests with leaders at all levels within the MAD.

(3) OPSEC planning is accomplished through the five step OPSEC process. The process begins by identification of critical information. In dynamic situations, the steps may be revisited at any time to adjust to new threats or information. The five step process is:

(a) Identification of critical information and indicators

(b) Analysis of threats

(c) Analysis of vulnerabilities

(d) Assessment of risk

(e) Application of OPSEC countermeasures

(4) All MAD Marines will familiarize themselves and comply with references (a) through (f).

c. Coordinating Instructions

(1) OPSEC Planning and Execution. The operations staff (S-3) is responsible for assisting MAD personnel in planning and executing the command's OPSEC program.

(2) Relationship with Security and Intelligence. OPSEC is neither a security nor an intelligence function. Security functions prevent unauthorized access to personnel, equipment, facilities, materials, and documents. Intelligence activities provide information on adversary forces, governments, and intentions. Counter-intelligence is information gathered and activities conducted to protect against espionage, other intelligence activities, sabotage, or assassinations conducted by, or on behalf, of foreign governments or elements thereof. OPSEC and these activities often overlap, and are mutually supportive. Close coordination must be maintained between all staff functions to ensure adequate OPSEC protection.

(3) OPSEC Program Managers and Coordinators. Program Managers are personnel who have OPSEC duties as their primary job. Coordinators are personnel who perform OPSEC functions as an additional duty. The MAD will appoint an OPSEC Coordinator to fulfill unit OPSEC responsibilities.

(4) Training Requirements

(a) The OPSEC Coordinator will complete an OPSEC fundamentals course within thirty (30) days of appointment. The course is listed as "IOSS CBT" and is available at the Navy Information Operations Command website: https://www.nioc-norfolk.navy.mil/opsec/index.html.

(b) The minimum OPSEC new-join and annual training requirements for all MAD personnel are:

1. A definition of OPSEC and its relationship to the command's security and intelligence programs.

2. An overview of the OPSEC process.

3. The command's current critical information list. This will ensure command members do not inadvertently disclose critical information. If the list is classified, then this requirement is waived for personnel without the appropriate security clearance and access. In such a case, unclassified examples will be provided in order to educate the command members on the general types of information they should not divulge. Enclosure (1) provides a list of the command's critical information.

4. A listing of personnel fulfilling OPSEC responsibilities within the command.

(5) Unclassified Website OPSEC

(a) Unclassified, publicly available websites are important to maintaining ties with the community and the American people; however, they present a potential risk to personnel, assets, and operations if inappropriate information is published on them. The MAD OPSEC Coordinator will review the MAD's website to ensure that no critical information is published via information, graphics, or photographs. In addition, as directed in reference (f), the following guidance is provided:

(b) Unclassified, publicly available websites shall not include classified material, "For Official Use Only" information, proprietary information, or information that could enable the recipient to infer this type of information. This includes, but is not limited to, lessons learned or maps with specific locations of sensitive units, ship battle orders, threat condition profiles, etc., activities or information relating to ongoing criminal investigations into terrorist acts, force protection levels, specific force protection measures being taken or number of personnel involved, plans of the day, or plans of the month. When it is necessary to gain release authority from a senior in the chain of command, subordinate commands will submit material for clearance only after it has been reviewed and necessary amendments made to the fullest capability of the submitting command.

(c) Unclassified, publicly available websites shall not display personnel lists, "roster boards", organizational charts, or command staff directories which show individuals' names, phone numbers, or email addresses which contain the individuals' name. General telephone numbers and non-personalized e-mail addresses for commonly requested resources, services, and contacts, without the individuals' names, are acceptable. The names, telephone numbers and personalized, official e-mail addresses of command/activity public affairs personnel and/or those designated by the commander as command spokespersons may be included in otherwise non-personalized directories.

(d) Biographies of general officers, commanders, commanding officers, officers in command, executive officers or deputies, the civilian equivalents of those officers just listed, and master gunnery sergeants or sergeants major may be posted to command unclassified, publicly-available websites. However, biographies published on unclassified, publicly-accessible websites will not include date of birth, current residential location, nor any information about family members.

(6) Public Affairs. Public Affairs is important in garnering public support, fostering community relations, and helping with the success of military operations. Public knowledge of military operations is inevitable because of advanced technology and instant media coverage. Therefore, Public Affairs staff must be included in the OPSEC planning process where media attention is expected or desired. The need for OPSEC should not be used as an excuse to deny non-critical information to the public.

(7) Family. OPSEC concerns will be addressed as part of the Unit & Personnel Family Readiness Program and stress the family's ability to contribute to protection of the command's critical information. Additionally, a family-focused OPSEC brochure will be distributed to all personnel upon joining the command.

(8) Quarterly OPSEC Working Group. The MAD shall convene an OPSEC working group at least quarterly to assist the OPSEC Coordinator in applying the OPSEC process to the MAD. Specific requirements for the convening of a working group can be found in enclosure (4) of reference (d).

(9) Inspections

(a) OPSEC is a functional area on the Commanding General's Checklist and will be evaluated as part of the Commanding General's Inspection Program.

(b) The MAD will conduct an annual, command-level OPSEC assessment.

(10) Response to Suspected Violations

(a) If a violation of command OPSEC procedures is suspected, command personnel will immediately attempt to remove and isolate the offending information from further public disclosure. All suspected violations will be reported to the OPSEC Program Coordinator for review.

(b) The OPSEC Program Coordinator will report any findings to the Executive Officer, and will provide recommendations for mitigating disclosures of critical information. Potential recommendations may include but are not limited to the removal of the critical information from further disclosure, remediation training for command personnel, or engaging local security personnel for further action.

(11) Excessive OPSEC. Excessive OPSEC can degrade operational effectiveness by interfering with activities such as coordination, training, and logistical support. Military operations are inherently risky, and the commander must evaluate each activity and operation and then balance required OPSEC measures against operational needs. Using the OPSEC process will help leaders to assess the risk and to apply appropriate OPSEC measures.

4. Administration and Logistics

a. Marine Corps OPSEC Support Element. Reference (e) directs each service to provide for an OPSEC support element. For the Marine Corps, this function is being provided by the Navy Information Operations Command's OPSEC Support Element. Additional assistance with OPSEC tactics, techniques and procedures, training support, advice for command level OPSEC assessments, or OPSEC aids such as posters should contact: https://www.navifor.usff.navy.mil/opsec/ or the organizational mailbox, opsec@navy.mil.

b. Definitions

(1) OPSEC Process. OPSEC planning is accomplished through the OPSEC process. This has five steps which are usually applied in a sequential order. In dynamic situations, the steps may be revisited at any time to adjust to new threats or information. The OPSEC Process steps are:

(a) Identification of Critical Information.

(b) Analysis of Threats.

(c) Analysis of Vulnerabilities.

(d) Assessment of Risk.

(e) Application of OPSEC Measures.

(2) OPSEC Indicator. These are friendly detectable actions and open sources of information that adversary intelligence systems can potentially detect or obtain and then interpret to derive friendly critical information. There are five basic characteristics to an OPSEC indicator that make them potentially useful for deriving critical information.

(a) Signature. The characteristic of an indicator that makes it identifiable or causes it to stand out.

(b) Association. The relationship of an indicator to other information or activities.

(c) Profile. The sum of an activity's unique signatures and associations.

(d) Contrasts. Differences observed between an activity's standard profile and current or recent activities.

(e) Exposure. When and for how long an indicator is observed.

(3) OPSEC Vulnerability. This is a condition in which friendly actions provide OPSEC indicators that may be obtained and accurately evaluated by an adversary in time to provide for a basis for effective adversary decision-making.

(4) OPSEC Measures. These are actions taken to reduce the probability of an enemy from either collecting OPSEC indicators or to correctly analyze their meaning.

(5) OPSEC Assessments. An OPSEC assessment is an examination of an operation or activity to determine if adequate protection from adversary intelligence exploitation exists. The OPSEC assessment is used to verify the effectiveness of OPSEC measures and determine if critical information is being protected. An assessment cannot be deducted until after critical information has been identified. Without understanding the critical information which should be protected, there can be no specific determination that OPSEC vulnerabilities exist.

(6) Critical Information and its relationship to Essential Elements of Friendly Information (EEFI)

(a) Critical Information is a term used throughout the OPSEC community and refers to "specific facts about friendly intentions, capabilities, and activities vitally needed by adversaries for them to plan and act effectively so as to guarantee failure or unacceptable consequences for friendly mission accomplishment."

(b) EEFI is a term used extensively throughout the Marine Corps and is defined as "key questions likely to be asked by adversary officials and intelligence systems about specific friendly intentions, capabilities, and activities, so they can obtain answers critical to their operational effectiveness."

(c) These two terms are very similar: the difference in the terms is their specificity. EEFIs are more general in nature and thought of in terms of a question, while critical information is more specific and thought of as the answer to the question. For example, a tactical situation would have "Time for Unit X to cross the Line of Departure" as an EEFI, while "0400" would be the specific fact (answering the EEFI) and therefore would represent critical information.

5. Command and Signal

a. Command

(1) This order applies to all military personnel assigned to the MAD.

(2) Any changes, additions, or modifications will be published via the MAD plan of the month.

b. Signal. This order is effective upon the date signed.

J. W. EGGSTAFF

MARINE AVIATION DETACHMENT CRITICAL INFORMATION LIST

Detailed facility maps or installation overhead photography with annotation of command or sensitive areas with greater resolution than is commercially available.

Government personnel information that would reveal force structure and readiness levels.

Force protection specific capabilities or response protocols.

Command leadership and VIP calendars, agendas, reservations, plans/routes, etc.

Vulnerabilities in command processes, disclosure of which could allow circumvention of security, financial, personnel safety, or operations procedures.

Details of emergency plans, evacuation, and recall procedures.

Personal identifying information.

Network user IDs and computer passwords.

Any material designated Controlled Unclassified Information (CUI), such as that marked For Official Use Only (FOUO).

Compilations of information that directly disclose information contained in this critical information list.

Details regarding military operations, missions, and exercises.

FOR OFFICIAL USE ONLY

MARINE AVIATION DETACHMENT CRITICAL INDICATORS LIST

OPSEC indicators are those friendly detectable actions and open-source information that can be interpreted or pieced together by an adversary to derive critical information.

Marine Aviation Detachment (MAD) OPSEC indicators can be characterized as:

Actions, information, or material indicating the levels of manning, readiness, and experience of personnel and/or units.

Stereotyped patterns in performing the mission that reveal the sequence of specific actions or when and how they are accomplished.

Unusual visible security imposed on particular efforts that highlight their significance.

Information indicating the presence of unusual types of units or systems, or unusual presence of personnel with special skills.

Internet-based broadcasting of movements, capabilities, locations, personnel, etc.

Internet-based posting of photos with sensitive information in the background.

Internet-based posting of sensitive documents, or filenames and tags with sensitive data in the name.

FOR OFFICIAL USE ONLY

POTENTIAL COUNTERMEASURES LIST

The following OPSEC countermeasures are examples only and are provided in order to generate ideas as Marines develop their own OPSEC countermeasures. Development of specific OPSEC countermeasures is as varied as the specific vulnerabilities that are designed to offset. These could include operational and logistical measures, technical measures, administrative measures, and operations and military deception measures.

a. Randomize the performance of functions and operational missions. Avoid repetitive or stereotyped tactics and procedures for executing operations and activities in terms of time, place, event, sequencing, formations, and command and control arrangements.

b. Limit non-secure computer e-mail messages to nonmilitary activities. Do not provide operational information in on-secure e-mail messages.

c. Prepare for computer network attack by ensuring patches are installed in a timely manner, data is backed up to devices not connected to the network, and redundant communication means and procedures are in place.

d. Use encryption to protect voice, data, and video communications.

e. Avoid bulletin board notices, plans of the day, or planning schedule notices that reveal when events will occur (or other specific details).

f. Conceal budgetary transactions, supply requests and actions and arrangements for services that reveal preparations or intention for operations.

g. Conceal the issuance of orders, the movement of special personnel and/or equipment to units, and the addition of special capabilities to units.

h. Control trash disposal and other housekeeping functions to conceal the identity and location of units, and other details pertaining to the operation.

i. Follow normal leave and liberty policies to the maximum extent possible to present a sense of normalcy.

j. Ensure that personnel discreetly prepare for their family's welfare in their absence and that their families are sensitized to a potentially abrupt departure.

k. Limit non-secure telephone conversations with non-military activities.

l. Provide family OPSEC briefs to inform family members of the need for OPSEC.

m. Ensure personnel are aware of OPSEC vulnerabilities presented by online social networking and avoid posting information about changes in personal or unit routines that could indicate operation planning or other details. Operational details in online forums both during and after a deployment should also be carefully avoided, so as not to put personnel in current or future rotations or operations at risk.

n. Ensure adequate policies and procedures are in place for shredding documents.

o. Ensure personnel understand the do's and don'ts of posting information on social network sites.

p. Ensure personnel are aware of the privacy setting of their social network sites.

q. Ensure administrators of the unit's public facing website is properly trained on public release and web risk assessment.

r. Ensure administrators of the unit's public facing website is conducting periodic website assessments for critical information, to include photos with critical information.

You are a vital player in our success!

As a family member of the military and civilian community, you are a vital player in our success, and we could not do our job without your support. You may not know it, but you also play a crucial role in ensuring your loved ones safety just by what you know of the military or government's day-to-day operations. You can protect your loved ones by protecting the information that you know. This is known as Operations Security or, OPSEC.

OPSEC is a vital element in protecting missions, service members and government personnel. Each and every one of us plays a vital role in ensuring we deny our adversaries potentially useful information.

We cannot afford to let our guard down whether we are on or off duty. Your diligence in OPSEC is key to ensuring our effectiveness in operations and our collective safety.

What can you do?

There are many countries and organizations that would like to harm Americans and degrade our influence in the world. It is possible and not unprecedented for family members of Department of Defense personnel to be targeted for intelligence collection. This is true in the United States and especially true overseas! Therefore, what you can do is be vigilant.

Thank you!

Thank you for taking the time to read this guide. Our goal is to provide you with a greater understanding of our security concerns. The information in this guide is not intended to make you paranoid or suspicious that everyone you meet is a secret agent or terrorist. Nevertheless, stay alert – if any stranger shows excessive interest in the affairs of you or your family members notify the authorities.

Questions

OPSEC Team (301) 342-3013 /
(301) 757-9834

Naval Criminal Investigative
Service (301) 342-3237

NAWCAD
(A0N0000)

OPSEC

OPERATIONS SECURITY

A guide for the family

From your OPSEC friend

"See Something, Say Something!"

OPSEC IS A FAMILY AFFAIR

All family members are part of the OPSEC team and need to protect the Navy's information to ensure our safety. ***Discuss OPSEC with the rest of your family!***

ENCLOSURE (4)

What is OPSEC?

OPSEC is keeping potential adversaries from discovering our critical information. As the name suggests, it protects our operations – planned, in progress and those completed. Success depends on secrecy and surprise, so the military can accomplish the mission quicker and with less risk. Enemies of freedom want our information, and they are not just after the military member to get it. They want you, the family member.

BE ALERT

Foreign Governments and organizations can collect significant amounts of useful information by using spies. A foreign agent may use a variety of approaches to befriend someone and get sensitive information. This sensitive information can be critical to the success of a terrorist or spy, and consequently deadly to Americans.

BE CAREFUL

There may be times when your family member cannot talk about the specifics of his or her job. It is very important to conceal and protect certain information such as flight schedules, ship movements, travel locations, and installation activities, just to name a few. Something as simple as a phone discussion concerning where your family member is going on travel or deploying to can be very useful to our adversaries.

Protecting Critical Information

Even though this information may not be secret, it is what we call "critical information." Critical Information deals with facts about military intentions, capabilities, operations or activities. If an adversary knew this detailed information, our mission accomplishment and personnel safety could be jeopardized. It must be protected to ensure an adversary does not gain a significant advantage.

By being a member of the military or civilian family, you will often know some bits of critical information. Do not discuss them outside of your immediate family and especially not over the telephone.

Examples of critical information:

- Detailed information about missions, projects or program platform.
- Details concerning locations and times of unit deployments.
- Personnel transactions that occur in large numbers (e.g. pay information, power of attorney, wills, deployment information).
- References to trend in unit morale or personnel problems.
- Personally Identifiable Information (e.g. SSN, DOB).

Puzzle pieces

These bits of information may seem insignificant. However, to a trained adversary, they are small pieces of a puzzle that highlight what we are doing and planning. Remember, the elements of security and surprises are vital to the accomplishment of our goals and our collective personnel protection.

Where and how you discuss this information is just as important as with whom you discuss it. Adversary's agents tasked with collecting information frequently visit some of the same stores, clubs, recreational areas or places of worship as you do.

Determined individuals can easily collect data from personal web pages. In addition, with inexpensive receivers available from electronics stores, they can also collect from cordless and cellular phones, and even baby monitors.

If anyone, especially a foreign national, persistently seeks information, notify the local Operations Security Office immediately or have your sponsor do it.

ENCLOSURE (4)