U.S. NAVY NTTP 3-13.3M

U.S. MARINE CORPS MCTP 3-32B

OPERATIONS SECURITY (OPSEC)

EDITION SEPTEMBER 2017

DISTRIBUTION RESTRICTION:
APPROVED FOR PUBLIC RELEASE;
DISTRIBUTION IS UNLIMITED.

NAVY WARFARE DEVELOPMENT COMMAND
1528 PIERSEY STREET, BLDG O-27
NORFOLK, VA 23511-2723

PRIMARY REVIEW AUTHORITY:
NAVAL INFORMATION WARFIGHTING
DEVELOPMENT COMMAND

URGENT CHANGE/ERRATUM RECORD		
NUMBER	DATE	ENTERED BY

DEPARTMENT OF THE NAVY
OFFICE OF THE CHIEF OF NAVAL OPERATIONS
HEADQUARTERS, U.S. MARINE CORPS

This and other Navy Warfare Library publications, including any edition updates, are available at the Navy Doctrine Library System Web sites: https://ndls.nwdc.navy.mil/default.aspx and https://portal.nwdc.navy.smil.mil/NDLS/default.aspx.

0411LP1179644

INTENTIONALLY BLANK

DEPARTMENT OF THE NAVY
NAVAL INFORMATION WARFIGHTING DEVELOPMENT CENTER
7941 BLANDY ROAD BUILDING NH-139
NORFOLK, VA 23551-2419

September 2017

LETTER OF APPROVAL

1. NTTP 3-13.3M/MCTP 3-32B (SEP 2017), Operations Security (OPSEC), is UNCLASSIFIED. Handle in accordance with the administrative procedures contained in NTRP 1-01 (MAY 2014), The Navy Warfare Library.

2. NTTP 3-13.3M/MCTP 3-32B (SEP 2017) is effective upon receipt and supersedes NTTP 3-54M/MCWP 3-40.9 (MAR 2009), Operations Security (OPSEC). Destroy superseded material without report.

3. NTTP 3-13.3M/MCTP 3-32B (SEP 2017) is the Department of the Navy's comprehensive operations security guide that provides commanders a method to incorporate the OPSEC process into daily activities, exercises, and mission planning to assist Navy and Marine Corps commands, afloat and ashore, in practicing and employing OPSEC.

4. NTTP 3-13.3M/MCTP 3-32B (SEP 2017) is approved for public release; distribution is unlimited.

J. A. WATKINS

NTTP 3-13.3M/MCTP 3-32B (SEP 2017), Operations Security (OPSEC), was developed in accordance with NTRP 1-01 (MAY 2014), The Navy Warfare Library, and has been reviewed for consistency with approved joint and Navy Service terminology. NTTP 3-13.3M/MCTP 3-32B (SEP 2017) is hereby promulgated as authoritative Navy and Marine Corps Service doctrine for use during operations and exercises and to serve as the basis for training operating forces and personnel.

Robert S. Walsh

ROBERT S. WALSH
Lieutenant General, U.S. Marine Corps
Deputy Commandant for Combat
Development and Integration

M. A. HITCHCOCK
Rear Admiral, U.S. Navy
Commander
Navy Warfare Development Command

INTENTIONALLY BLANK

September 2017

PUBLICATION NOTICE

ROUTING

1. NTTP 3-13.3M/MCTP 3-32B (SEP 2017), OPERATIONS SECURITY (OPSEC), is available in the Navy Warfare Library. It supersedes and cancels NTTP 3-54M/MCWP 3-40.9 (MAR 2009), OPERATIONS SECURITY (OPSEC) and is effective upon receipt.

2. Summary. NTTP 3-13.3M/MCTP 3-32B is the Department of the Navy comprehensive OPSEC guide that provides commanders a method to incorporate the OPSEC process into daily activities, exercises, and mission planning to assist Navy and Marine Corps commands, afloat and ashore, in practicing and employing OPSEC.

____
____
____
____
____
____
____
____
____
____

____
Navy Warfare Library Custodian

Navy Warfare Library publications must be made readily available to all users and other interested personnel within the U.S. Navy.

Note to Navy Warfare Library Custodian

This notice should be duplicated for routing to cognizant personnel to keep them informed of changes to this publication.

INTENTIONALLY BLANK

CONTENTS

Page No.

CHAPTER 1—INTRODUCTION

CHAPTER 2—OPERATIONS SECURITY

CHAPTER 3—OPSEC PROCESS

CHAPTER 4—THE OPSEC ASSESSMENT

Page No.

CHAPTER 5—OPSEC'S ROLE IN OPERATIONAL MESSAGES

CHAPTER 6—WEB RISK ASSESSMENT AND WEB SITE REGISTRATION

CHAPTER 7—NAVAL CRIMINAL INVESTIGATIVE SERVICE CONTRIBUTIONS TO THE OPSEC PROCESS

Page No.

CHAPTER 8—THE OPSEC PROGRAM MANAGER AND PUBLIC AFFAIRS OFFICER RELATIONSHIP

CHAPTER 9—OPSEC GUIDANCE FOR THE NAVY OMBUDSMAN AND MARINE CORPS FAMILY READINESS OFFICER

CHAPTER 10—SOCIAL MEDIA

CHAPTER 11—OPSEC PLANNING

Page No.

LIST OF ILLUSTRATIONS

Page No.

CHAPTER 2—OPERATIONS SECURITY

CHAPTER 3—OPSEC PROCESS

CHAPTER 4—THE OPSEC ASSESSMENT

CHAPTER 6—WEB RISK ASSESSMENT AND WEB SITE REGISTRATION

CHAPTER 8—THE OPSEC PROGRAM MANAGER AND PUBLIC AFFAIRS OFFICER RELATIONSHIP

APPENDIX A—OPSEC CHECKLISTS

APPENDIX C—CRITICAL INFORMATION LIST

APPENDIX F—THREAT AND VULNERABILITY ANALYSIS

Page No.

APPENDIX G—RISK ANALYSIS AND COUNTERMEASURE CONSIDERATIONS

APPENDIX K—WEB SITE SELF-ASSESSMENT CHECKLIST

APPENDIX M—OMBUDSMAN AND FAMILY READINESS OFFICER GUIDANCE

APPENDIX O—DECISION FLOW CHART

PREFACE

NTTP 3-13.3M/MCTP 3-32B is the Department of the Navy comprehensive OPSEC guide that provides commanders a method to incorporate the OPSEC process into daily activities, exercises, and mission planning to assist Navy and Marine Corps commands, afloat and ashore, in practicing and employing OPSEC.

Unless otherwise stated, masculine nouns and pronouns do not refer exclusively to men.

Report administrative discrepancies by letter, message, or e-mail to:

COMMANDER
NAVY WARFARE DEVELOPMENT COMMAND
ATTN: DOCTRINE
1528 PIERSEY STREET, BLDG O-27
NORFOLK, VA 23511-2723

NWDC_NRFK_FLEETPUBS@NAVY.MIL

ORDERING PRINTED COPIES

Order printed copies of a publication using the print-on-demand (POD) system. A command may requisition a publication using the standard military standard requisitioning and issue procedure (MILSTRIP) process on the Naval Supply Systems Command Web site called the Naval Logistics Library (https://nll.ahf.nmci.navy.mil). An approved requisition is forwarded to the specific Defense Logistics Agency (DLA) site at which the publication's electronic file is officially stored. Commands may also order publications through the Navy Doctrine Library System Web site (https://ndls.nwdc.navy.mil/default.aspx) by visiting publication-specific metadata Web pages and selecting the hyperlink on the stock number, which is linked to the Naval Logistics Library Web site. Users may be prompted to create an account to complete the ordering process. Currently, three copies are printed at no cost to the requester.

CHANGE RECOMMENDATIONS

Procedures for recommending changes are provided below.

WEB-BASED CHANGE RECOMMENDATIONS

Recommended changes to this publication may be submitted to the Navy Doctrine Library System, accessible through the Navy Warfare Development Command (NWDC) Web site at: https://ndls.nwdc.navy.mil/default.aspx or https://portal.nwdc.navy.smil.mil/NDLS/default.aspx.

URGENT CHANGE RECOMMENDATIONS

When items for changes are considered urgent, send this information by message to the primary review authority, info NWDC. Clearly identify and justify both the proposed change and its urgency. Information addressees should comment as appropriate. See the sample for urgent change recommendation message format on page 17.

ROUTINE CHANGE RECOMMENDATIONS

Submit routine recommended changes to this publication at any time by using the routine change recommendation letter format on page 18. Mail it to the address below or post the recommendation on the Navy Doctrine Library System site.

COMMANDER
NAVY WARFARE DEVELOPMENT COMMAND
ATTN: DOCTRINE
1528 PIERSEY STREET, BLDG O-27
NORFOLK, VA 23511-2723

CHANGE BARS

Revised text is indicated by a black vertical line in the outside margin of the page, like the one printed next to this paragraph. The change bar indicates added or restated information. A change bar in the margin adjacent to the chapter number and title indicates a new or completely revised chapter.

WARNINGS, CAUTIONS, AND NOTES

The following definitions apply to warnings, cautions, and notes used in this manual:

⚠ **WARNING**

An operating procedure, practice, or condition that may result in injury or death if not carefully observed or followed.

⚠ **CAUTION**

An operating procedure, practice, or condition that may result in damage to equipment if not carefully observed or followed.

Note

An operating procedure, practice, or condition that requires emphasis.

WORDING

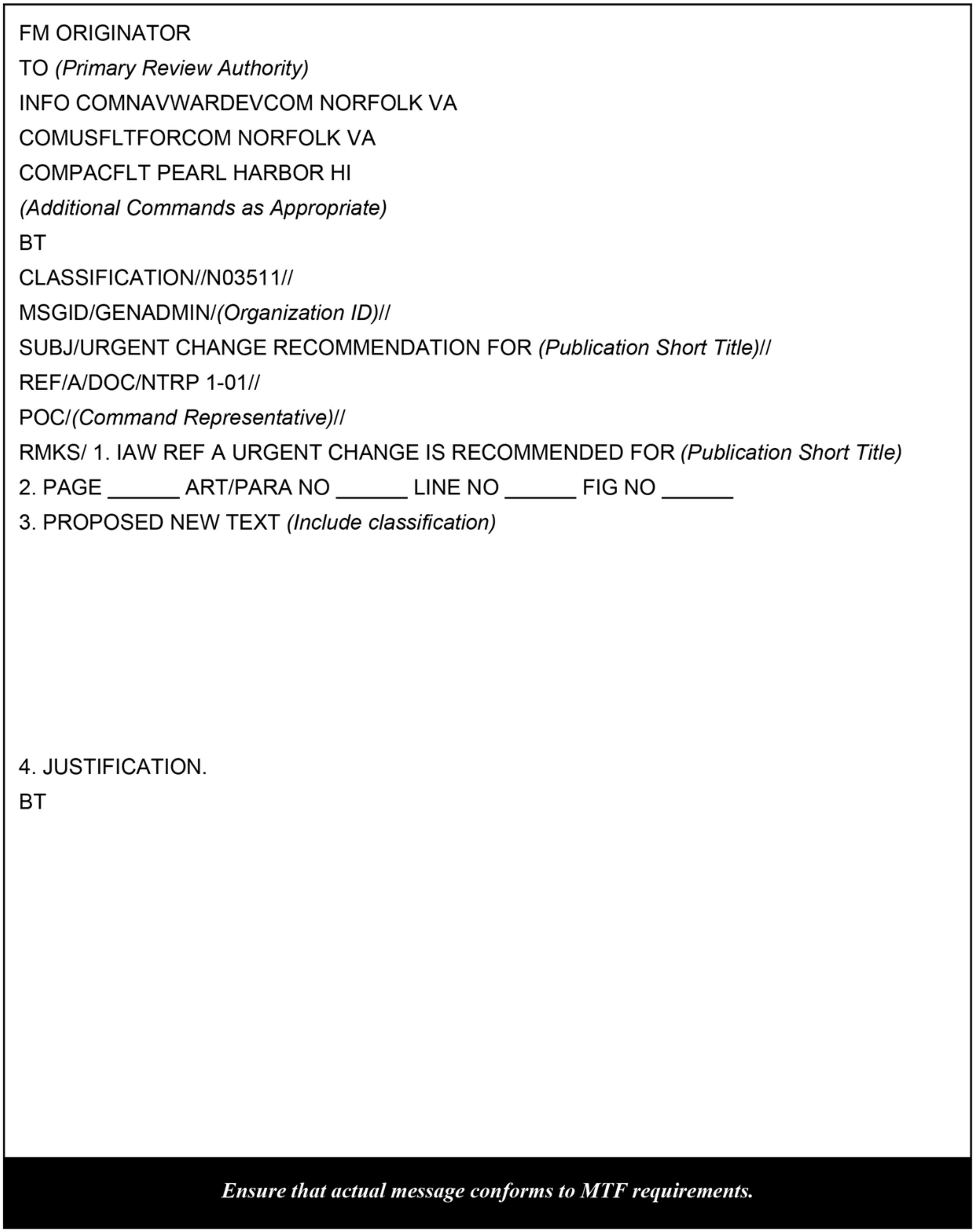
Word usage and intended meaning throughout this publication are as follows:

“Shall” indicates the application of a procedure is mandatory.

“Should” indicates the application of a procedure is recommended.

“May” and “need not” indicate the application of a procedure is optional.

“Will” indicates future time. It never indicates any degree of requirement for application of a procedure.

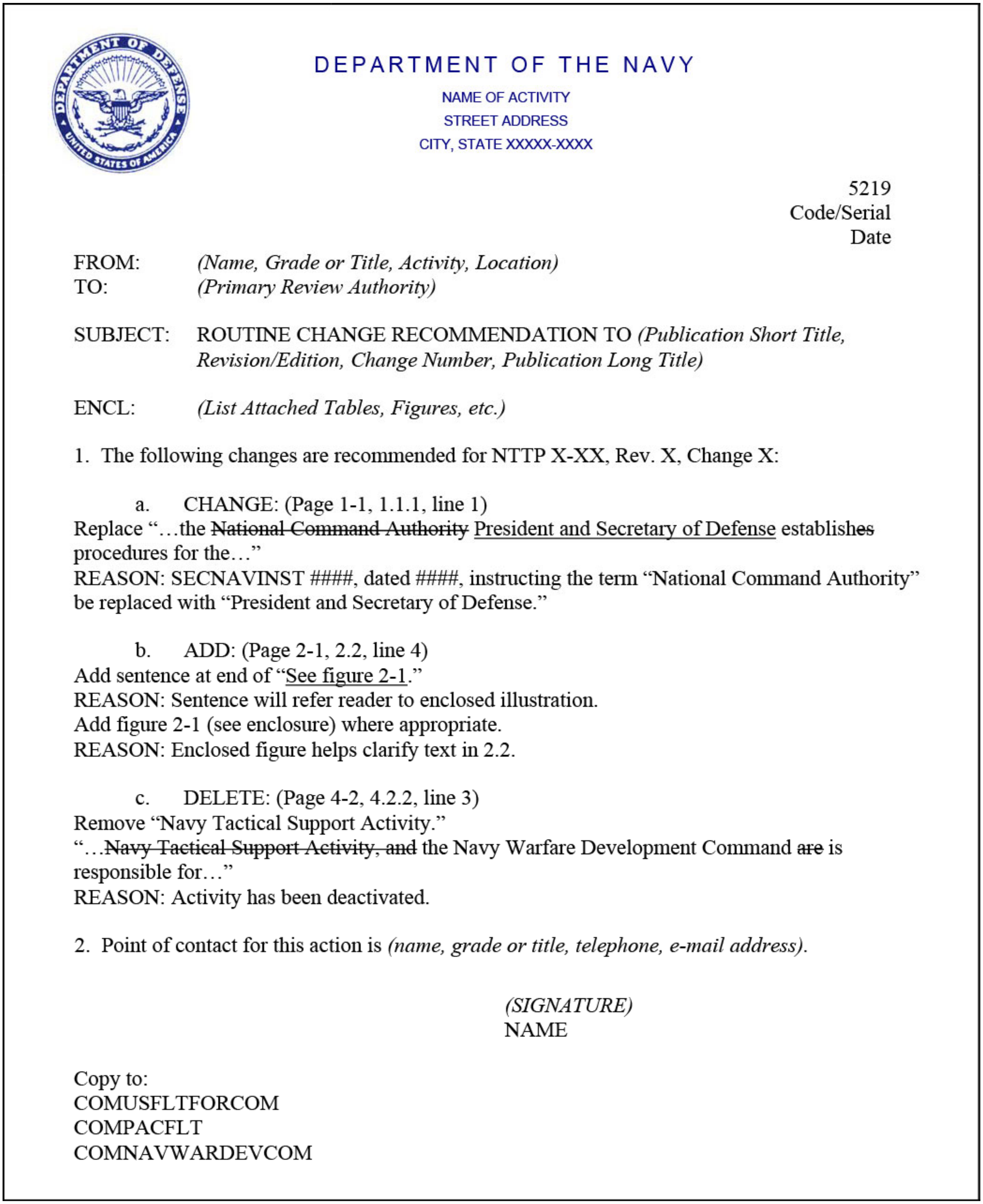


FM ORIGINATOR
TO *(Primary Review Authority)*
INFO COMNAVWARDEVCOM NORFOLK VA
COMUSFLTFORCOM NORFOLK VA
COMPACFLT PEARL HARBOR HI
(Additional Commands as Appropriate)
BT
CLASSIFICATION//N03511//
MSGID/GENADMIN/*(Organization ID)*//
SUBJ/URGENT CHANGE RECOMMENDATION FOR *(Publication Short Title)*//
REF/A/DOC/NTRP 1-01//
POC/*(Command Representative)*//
RMKS/ 1. IAW REF A URGENT CHANGE IS RECOMMENDED FOR *(Publication Short Title)*
2. PAGE ______ ART/PARA NO ______ LINE NO ______ FIG NO ______
3. PROPOSED NEW TEXT *(Include classification)*

4. JUSTIFICATION.
BT

Ensure that actual message conforms to MTF requirements.

Urgent Change Recommendation Message Format



DEPARTMENT OF THE NAVY
NAME OF ACTIVITY
STREET ADDRESS
CITY, STATE XXXXX-XXXX

5219
Code/Serial
Date

FROM: *(Name, Grade or Title, Activity, Location)*
TO: *(Primary Review Authority)*

SUBJECT: ROUTINE CHANGE RECOMMENDATION TO *(Publication Short Title, Revision/Edition, Change Number, Publication Long Title)*

ENCL: *(List Attached Tables, Figures, etc.)*

1. The following changes are recommended for NTTP X-XX, Rev. X, Change X:

a. CHANGE: (Page 1-1, 1.1.1, line 1)
Replace "…the ~~National Command Authority~~ President and Secretary of Defense establish~~es~~ procedures for the…"
REASON: SECNAVINST ####, dated ####, instructing the term "National Command Authority" be replaced with "President and Secretary of Defense."

b. ADD: (Page 2-1, 2.2, line 4)
Add sentence at end of "See figure 2-1."
REASON: Sentence will refer reader to enclosed illustration.
Add figure 2-1 (see enclosure) where appropriate.
REASON: Enclosed figure helps clarify text in 2.2.

c. DELETE: (Page 4-2, 4.2.2, line 3)
Remove "Navy Tactical Support Activity."
"…~~Navy Tactical Support Activity, and~~ the Navy Warfare Development Command ~~are~~ is responsible for…"
REASON: Activity has been deactivated.

2. Point of contact for this action is *(name, grade or title, telephone, e-mail address)*.

(SIGNATURE)
NAME

Copy to:
COMUSFLTFORCOM
COMPACFLT
COMNAVWARDEVCOM

Routine Change Recommendation Letter Format

CHAPTER 1

Introduction

1.1 PURPOSE

In 1988, President Ronald Reagan signed national security decision directive (NSDD) 298, establishing a national operations security (OPSEC) program and creating a national OPSEC structure. NSDD 298 requires each Federal agency or organization supporting national security missions with classified or sensitive activities to establish an OPSEC program. Due to the Department of the Navy's (DON) inherent national security mission and use of classified and sensitive information, NSDD 298 serves to inform the DON OPSEC program. OPSEC is a formal program which identifies and protects both sensitive unclassified and classified information that ensures mission success. This document provides relevant U.S. Navy and Marine Corps tactics, techniques, and procedures from myriad reference materials to assist the command OPSEC program manager, and ultimately the commander, in taking prudent OPSEC considerations into account during day-to-day activities and the mission planning process.

1.2 SCOPE

Navy tactics, techniques, and procedures (NTTP) 3-13.3M/Marine Corps tactical publication (MCTP) 3-32B provides commanders with an OPSEC overview, OPSEC evolution, and guidance for some of the most crucial aspects of OPSEC: that of identifying critical information, and recognizing the collection methods from potential adversaries. This document also explains the Department of Defense (DOD) OPSEC five-step process, the baseline of every OPSEC program. NTTP 3-13.3M/MCTP 3-32B addresses the areas of OPSEC and force protection; public affairs officer (PAO) interaction; the role of the U.S. intelligence community in coordination with OPSEC; the OPSEC, ombudsman, or family readiness officer (FRO) relationship; and the conducting of OPSEC assessments. This publication includes separate chapters and appendixes on Web risk assessment (WRA), OPSEC in contracts, OPSEC during fleet workups, and guidance to implement effective programs at the individual unit, strike group, and shore establishment levels.

1.3 BACKGROUND

NTTP 3-13.3M/MCTP 3-32B is the DON's comprehensive OPSEC guide, which provides commanders with methods for incorporating the OPSEC process into daily activities, exercises, and mission planning. Chief of Naval Operations instruction (OPNAVINST) 3430.26A of 30 August 2013, OPNAVINST 3432.1A of 04 August 2011, Marine Corps order (MCO) 3070.2A, Marine administrative message (MARADMIN) 071/04, and All Marines (ALMAR) 007/04 serve as the foundation for this publication. NTTP 3-13.3M/MCTP 3-32B integrates research materials and background derived from coordination and personal interviews with national OPSEC entities, joint personnel, echelons 1 through 4 command personnel, and other Service personnel. This publication incorporates information collected, lessons learned over many years of naval OPSEC afloat and ashore, and addresses newly emerging areas such as the use of social media and technical vulnerabilities of Web sites, and OPSEC training.

1.4 SUMMARY

The purpose of NTTP 3-13.3M/MCTP 3-32B is to assist Navy and Marine Corps commands, afloat and ashore, with practicing and employing OPSEC. This publication incorporates fleet and shore establishment input, and provides a practical planning process that integrates OPSEC into the daily routine and planning process. The publication allows all Navy and Marine personnel to access current information for planning and executing OPSEC in conjunction with all aspects of warfare and everyday activities, to include public life.

INTENTIONALLY BLANK

CHAPTER 2

Operations Security

2.1 OVERVIEW

OPSEC is a capability that identifies and controls critical information and indicators of friendly force actions attendant to military operations, and incorporates countermeasures to reduce the risk of an adversary exploiting vulnerabilities. When effectively employed, it denies or mitigates an adversary's ability to compromise or interrupt a mission, operation, or activity. Without a coordinated effort to maintain the essential secrecy of plans and operations, our enemies can forecast, frustrate, or defeat major military operations. Well-executed OPSEC helps to blind our enemies, forcing them to make decisions with insufficient information.

OPSEC is an information-related capability (IRC) that, when properly employed, can be used to gain advantages in the information environment, just as other military techniques are used in the operational environment. OPSEC fits into a web of many other mutually supporting IRCs, such as military deception, public affairs, and cyberspace operations. The effective application, coordination, and synchronization of other IRCs is a critical component of the execution of OPSEC and achievement of a common information operations (IO) objective. When used in concert with one another, OPSEC and other IRCs can be effectively integrated into operations to create operationally exploitable conditions necessary for achieving a commander's objectives.

OPSEC …

1. is an analytic process
2. focuses on adversary collection capability and intent
3. emphasizes the value of sensitive and critical information.

Every Navy and Marine Corps command performs a core, unclassified mission. Although unclassified, individual tasks required for a command to successfully accomplish its mission may contain information that—when pieced together with other unclassified information—reveal classified, sensitive or critical information. Its disclosure may lead to susceptibility to adversarial action. This process of piecing information together is known as data aggregation (see figure 2-1). OPSEC provides a means for screening information prior to its release in order to prevent aggregation with other information, ultimately revealing intentions or capabilities. Aggregation of information—with its potentially negative impact on operations, missions, activities, and personnel safety—is a basic OPSEC concept. It is incumbent upon commanders to incorporate OPSEC into all operations. Appendix A provides comprehensive OPSEC checklists to assist commands in executing OPSEC programs.

An effective OPSEC program has its chain of command's full support. Command emphasis includes an OPSEC program manager or coordinator being appointed in writing by the commanding officer, and an OPSEC working group charged with the responsibility of ensuring the command and family members maintain an acute OPSEC awareness (see appendix H).

While not a panacea for every operational challenge, if enacted properly, OPSEC measures can minimize the risk of compromising information that could assist our adversaries in degrading our mission effectiveness.

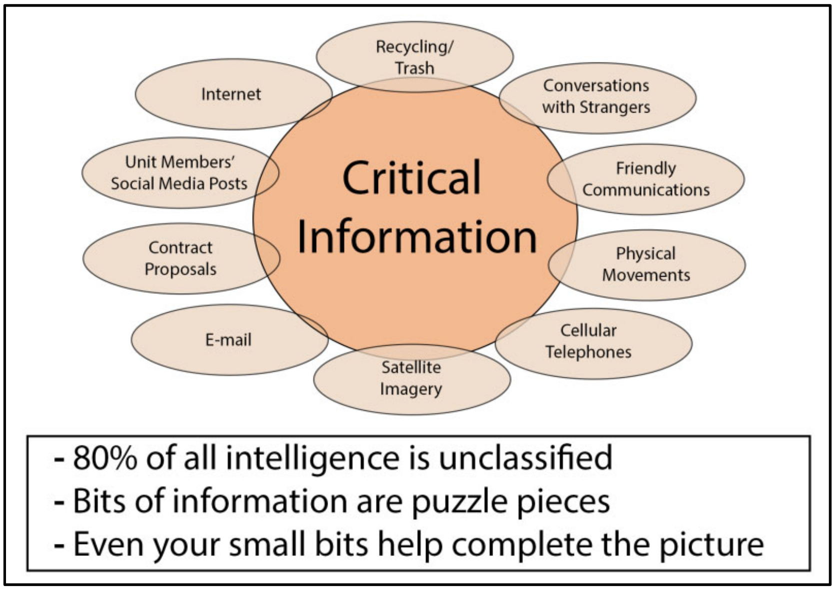

Recycling/ Trash
Internet
Conversations with Strangers
Unit Members' Social Media Posts
Critical Information
Friendly Communications
Contract Proposals
Physical Movements
E-mail
Cellular Telephones
Satellite Imagery
- 80% of all intelligence is unclassified
- Bits of information are puzzle pieces
- Even your small bits help complete the picture

Figure 2-1. Data Aggregation

Note

> OPSEC indicators are those friendly actions and open sources of information that adversary intelligence systems can potentially detect or obtain and then interpret to derive friendly critical information.

> "Even minutiae should have a place in our collection, for things of a seemingly trifling nature, when enjoined with others of a more serious cast, may lead to valuable conclusion."
>
> —*General Washington*

2.2 OPSEC CHARACTERISTICS

OPSEC does not have a fixed set of rules. It is a dynamic process and can change as the mission and its environment change. Information critical in one phase of the mission may not be critical in subsequent phases. Enemy intelligence threats faced in one battle may be different in the next. Vulnerabilities in one situation may not exist in another. Risk will vary as information criticality, threats, and vulnerabilities change independently and in relation to one another. Countermeasures that are effective in a specific situation may not work in other situations. Deception, a critical OPSEC countermeasure, rarely works against a specific enemy force more than once.

OPSEC integrates and mutually supports all traditional security disciplines (physical, information, cyber, personnel, technical, etc.) and is linked to other IRCs and other operational functions such as maneuver. OPSEC is a process developed to deny adversaries publicly available indicators that are generally unclassified, and it is not intended to replace traditional security programs created to protect classified information.

OPSEC is an operational function. Security, intelligence, and counterintelligence (CI) support its implementation. OPSEC program managers need expertise gained through formal training, and comprehensive exposure to the mission of the unit and application of the OPSEC process in order to choose the best course or courses of action needed to protect critical information. OPSEC is an operations enabler, not a prohibitor.

In a naval context, OPSEC is a command responsibility; the entire command trains, plans, executes OPSEC (see appendix L). It requires, at a minimum, operationally mature OPSEC-trained program managers capable of:

coordinating functions for the commander; advising the commander on the process, implementation, and OPSEC best practices; and recommending the best course of action as part of the "go/no-go" decision cycle. OPSEC program managers ensure all participants (planners, operators, etc.) are aware of relevant critical information and can coordinate timely, resourced solutions. OPSEC program managers and planners are most effective (particularly in planning for crises or contingencies) when they obtain support and assistance from OPSEC professionals thoroughly trained and experienced in applying the OPSEC process in a variety of settings.

2.3 EVOLUTION OF OPSEC

OPSEC, as a term, was coined in the late 1960s. The concept is, however, as old as the practice of warfare. OPSEC has been a fundamental element in virtually all of warfare throughout recorded history, and remains a key element in achieving both strategic and tactical surprise.

In the modern era, OPSEC was effective in conjunction with the deception plan leading up to and during execution of the Allied invasion of the northern European continent Operation OVERLORD on D-Day in 1944. Allied true intentions (i.e., to attack at Normandy vice Pas de Calais) were effectively masked, and false intentions were effectively portrayed. OPSEC and military deception were so effective that for as long as two days after the landing at Normandy, Hitler believed that the operation was a ruse and that the main attack would occur at Calais. This resulted in a slow Axis response because many enemy defensive forces were concentrated on Calais.

During the Vietnam War, U.S. forces initially underestimated both the enemy threat and our vulnerabilities to it. In late 1966 and early 1967, it became apparent through battle damage assessments and other sources that the North Vietnamese and Viet Cong were obtaining advance warnings of drone flights, B–52 Operation ARC LIGHT missions over South Vietnam, and tactical fighter-bomber Operation ROLLING THUNDER missions against North Vietnam. Counterintelligence and security personnel conducted investigations in order to find sources of leaked classified information under an effort that is known as Operation PURPLE DRAGON; however, no single point sources were found. Rather, a team of United States Pacific Command (USPACOM) operations and security analysts, after thoroughly examining virtually all aspects of the drone and bombing operations, determined that unclassified indicators throughout virtually all phases of mission planning and execution gave sufficient warning to the North Vietnamese and Viet Cong. Due to these indicators, enemy forces launched antiaircraft defenses and implemented passive defenses on the ground (such as vacating targeted areas), and destroyed roughly 75 percent of our drone aircraft, rendering bombing missions ineffective.

The USPACOM OPSEC team identified that Notices to Airmen concerning drone, ARC LIGHT and ROLLING THUNDER were routinely published and broadcast throughout the theater of operations. In particular, altitude clearances for ARC LIGHT missions (originating from Guam and Okinawa) coordinated openly with civil air traffic control entities throughout Southeast Asia more than 24 hours prior to mission launch. Based on disclosed altitudes, times, and locations for entry and exit of the flights into and out of the South Vietnam Air Defense Identification Zone, the enemy made reasonably accurate predictions as to where and when the strikes would take place. The need for forewarning was eliminated and the enemy's ability to deduce targets from entry and exit points was effectively neutralized through the initiation of permanent altitude reservations and entry and exit points.

Regarding ROLLING THUNDER strikes against North Vietnam, the OPSEC team found that predictable operating patterns for strike aircraft originating in Thailand gave away times and locations of attacks. Flights targeting some locations in North Vietnam required refueling while others did not. When refueling operations were required, refueling for specific targets took place at specific points. Radar easily detected and identified them by their nonchanging clear-text call signs well in advance of the refueling missions. Based on the time the refueling operations took place, the enemy made reasonably accurate predictions of where and when the strikes would take place.

Sent 24 hours in advance, formatted messages concerning the flights of the drone-carrying C-130s frequently compromised drone operations. Although these messages were manually encrypted, they were detectable through their uniqueness. Simple pattern analysis allowed the enemy to link these messages with drone flights. With the initiation of measures to mask the communications with online communications security (COMSEC) devices, drone loss rates dropped by 60 percent.

The National Security Agency found that at least two broadcast stations' alerting of B-52 strikes dropped significantly following the implementation of PURPLE DRAGON's recommendations on ARC LIGHT. During the first month of the PURPLE DRAGON survey (December 1966), the two North Vietnamese Army stations alerted 34 percent of ARC LIGHT missions, with an average warning time of 8 and a half hours. In April 1967, at the end of PURPLE DRAGON, the North Vietnamese Army alert broadcasts fell to only 5 percent of B-52 strikes, with an average alert time of less than 30 minutes.

As with most PURPLE DRAGON surveys during the Vietnam War, the OPSEC posture of the surveyed organizations improved at least temporarily, following the PURPLE DRAGON surveys of mobile riverine operations and Army ground operations. More importantly, however, evidence of the enemy's prior awareness of U.S. operations significantly decreased as the surveyed units implemented suggested changes in procedures. U.S. intercept of enemy alert messages dropped off, and contact with the enemy usually increased. These positive results, however, were almost invariably only temporary. In most cases, improved operations security of the units involved denied the enemy only one valuable source of foreknowledge of U.S. intentions and capabilities. The enemy would then cast about until they had found a new source of information to take its place. Then, evidence of the enemy's prior knowledge would again surface and the OPSEC procedure would begin again.

Following USPACOM's success of these initial OPSEC studies in 1967, a team was established within USPACOM (J-3). This team conducted approximately 55 additional OPSEC studies throughout the Pacific Theater. These studies continued to search out the compromise of critical information to enemy threats and recommend viable countermeasures that, when instituted, enhanced operational effectiveness. The Chairman of the Joint Chiefs of Staff (General Earle Wheeler) recognized the value of these studies and, in May 1968, proclaimed, "…the doctrinal approach which has been designed…will have broad application in military planning and operations in all theaters under all conditions of military operations." The Chairman directed all unified and specified commands to establish OPSEC programs.

In the following years, the military experienced OPSEC failures and successes. Operation EAGLE CLAW, the April 1980 attempt to rescue U.S. hostages in Iran, was a good example of too much emphasis on security and not enough on sharing operational information. In the name of security, key operators did not know what other key operators were planning. This caused confusion in planning and execution, and contributed to mission failure.

Conversely, Operation DESERT STORM planning and execution of the "left hook" of VII Corps to the west and Marine amphibious assault feint off the Kuwaiti coast were excellent examples of OPSEC (to hide VII Corps during preattack phase) and deception allowing coalition forces to achieve surprise.

In Kosovo, effectiveness of superior coalition firepower was frequently compromised due to nonsecure communications between planning elements as well as aircraft concerning targets. Targeting information was often passed in the clear in sufficient time for Serbian targets to relocate. The bottom line was that although we ultimately achieved victory, NATO forces flew far more sorties and expended far more ordinance than would have likely been needed with good OPSEC.

Many see the events of September 11, 2001 as either an Al-Qaeda success, or an OPSEC failure. The openness and complacency of our society permitted Al-Qaeda to thoroughly scrutinize our immigration practices, law enforcement procedures, intelligence capabilities and limitations, and aviation system procedures. These conditions allowed the terrorists to enter the United States, evade observation, obtain flight training, choose ideal aircraft (fully fueled, with light passenger loads), circumvent airport and aircraft security, and carry out at least 75 percent of their mission.

OPSEC needs to continue to mature as operations and exercises are integrated with coalition and allied partners. Information traditionally protected as OPSEC-sensitive is now shared with many partners, providing additional avenues for this information to become known to the general public. Commanders should consider the need to establish an OPSEC working group for Allied or coalition exercises and operations as early in planning as possible in order to establish OPSEC policy.

CHAPTER 3

OPSEC Process

3.1 SCOPE

The protection of essential elements of friendly information (EEFIs) and—subsequently—critical information, is essential to the success of the OPSEC process. Failure to recognize EEFI and critical information renders a commander ineffective against revealing operational- and mission-related vulnerabilities and, thus, to conducting risk assessments and enacting countermeasures against a real or potential threat. The OPSEC process, also known as the OPSEC five-step process, is the enabling vehicle for OPSEC planning (see figure 3-1). It provides the required information for the OPSEC portion of any plan or activity. A standing OPSEC program instruction that details how OPSEC is performed at a command should inform all OPSEC programs. See appendix E for an example of an OPSEC program instruction. This chapter takes the OPSEC program manager through the five-step process, providing comprehensive guidance to produce an effective OPSEC plan. Immediate superior in command (ISIC) OPSEC program managers provide OPSEC planning guidance to their subordinate units in order to ensure that all units operate under the same principles for a given area of operations (AO). All units must adhere to higher command guidelines in order to maximize OPSEC effectiveness. The five-step process is a proven method for safeguarding critical information. OPSEC planning must be closely coordinated with internal operations planning efforts and the planning of supported or supporting units. Applying the process during the planning phase of any event or operation greatly enhances the commander’s effectiveness in identifying and protecting critical information. Paragraphs 3.3 through 3.7 describe the five steps.

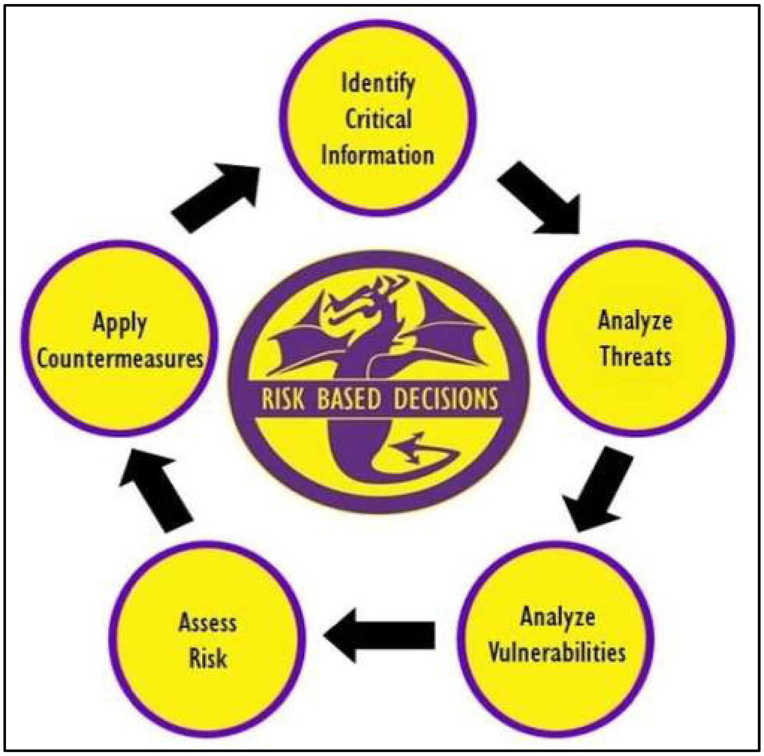


Figure 3-1. The OPSEC Process

3.2 ESSENTIAL ELEMENTS OF FRIENDLY INFORMATION

Planners need to establish EEFI (i.e., key questions adversaries will likely inquire about regarding our intentions, capabilities, and activities) in order to obtain answers critical to their own operational effectiveness. The answers to EEFI can potentially lead to critical information.

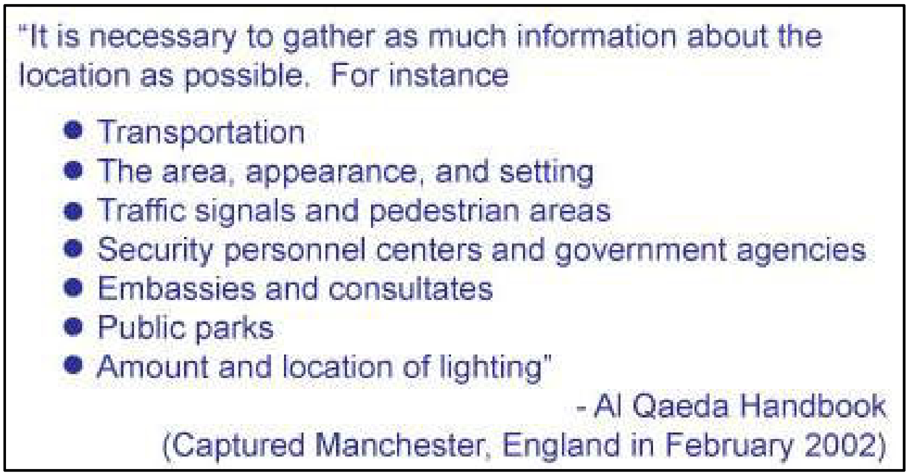
The commanding officer and staff seek to identify the questions they think the adversary will ask about friendly intentions, capabilities, and activities while they assess and compare friendly-versus-adversary capabilities during the environment awareness and shaping process for a specific operation or activity (as discussed in NTTP 3-13.2, Navy Information Operations Warfare Commander's Manual). Appendix B contains a generic list of questions, the answers to which may help the OPSEC program manager establish EEFI.

Note

> The successful application of OPSEC methodology depends upon the detailed and accurate identification of mission-related critical information. Since critical information is unique to the mission, compiling a single list of critical information for both the Navy and Marine Corps is impractical. However, it is feasible to create a generic list of critical information, giving commanders and OPSEC planners the flexibility to expand generic categories of critical information into an accurate program or project level list.

3.3 STEP ONE: IDENTIFY CRITICAL INFORMATION

Critical information is defined as information about friendly (U.S., allied, or coalition) activities, intentions, capabilities, or limitations that an adversary seeks in order to gain a military, political, diplomatic, economic, or technological advantage. Such information—if prematurely revealed to an adversary—may prevent or complicate mission accomplishment, reduce mission effectiveness, damage friendly resources, or cause loss of life. Critical information usually involves a few key elements of information concerning friendly activities or intentions that, if revealed to an adversary, may significantly degrade mission effectiveness. It should be noted, however, that information that is critical in one phase of the mission may not be critical in subsequent phases. Appendix C provides a template to assist an OPSEC program manager with identifying critical information and a list of generic critical information in the form of an "all hands" memorandum. Derived from EEFI, critical information includes only information that an adversary vitally needs. Identifying critical information focuses the remainder of the OPSEC process on protecting vital information, rather than attempting to protect all classified or sensitive information. Figures 3-2 and 3-3 depict examples of information considered critical to an adversary's success.

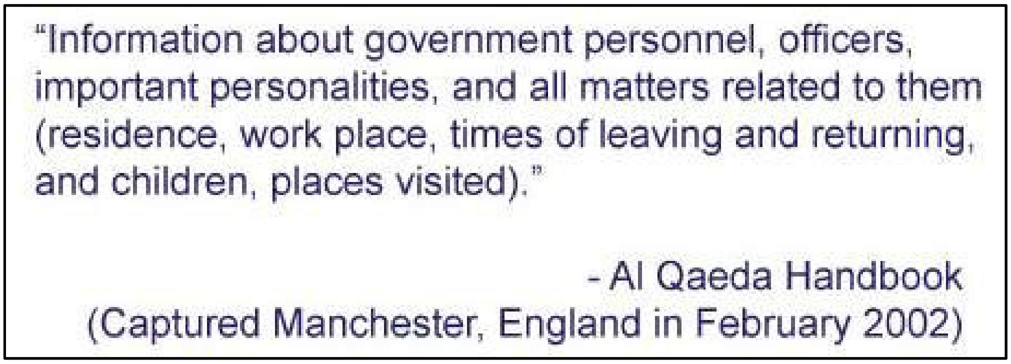


"It is necessary to gather as much information about the location as possible. For instance

- Transportation
- The area, appearance, and setting
- Traffic signals and pedestrian areas
- Security personnel centers and government agencies
- Embassies and consultates
- Public parks
- Amount and location of lighting"

- Al Qaeda Handbook
(Captured Manchester, England in February 2002)

Figure 3-2. Example of Critical Information



"Information about government personnel, officers, important personalities, and all matters related to them (residence, work place, times of leaving and returning, and children, places visited)."

- Al Qaeda Handbook
(Captured Manchester, England in February 2002)

Figure 3-3. Example of Critical Information

Critical information is listed in the OPSEC portion of an operation plan, operation order (OPORD), or command instruction. An example of an OPSEC instruction ((Tab C) to an IO plan (Appendix 3) to an operations order (Annex C)) is provided in appendix D.

OPSEC indicators must be considered along with critical information. OPSEC indicators are defined as friendly detectable actions and open source information that can be interpreted or pieced together to allow an adversary to obtain critical or sensitive information, or to identify vulnerabilities. An indicator can be looked at by itself or in conjunction with something else. There are five major characteristics of an OPSEC indicator. They are identified as signature, associations, profiles, contrasts, and exposure, or SAPCE. Signature is an indicator that makes something identifiable or causes it to stand out. An association is the relationship of an indicator to other critical information or activities. A profile is the signatures plus the associations. Adversaries look for patterns and signatures to establish a profile. Patterns are the way things are done, arranged, or have occurred. A contrast is the differences observed between an activity's standard profile and its most recent or current actions. Exposure is when and how long an indicator is observed. An example of an indicator may be an increase in the frequency of patrols in a specific area. The adversary may use this indicator to determine that a major operation is soon planned for that particular area. Various measures may be implemented to reduce the visibility of indicators or vulnerabilities. OPSEC indicators must also be taken into account when developing the initial critical information list.

Signature management is an important part of the OPSEC process. The characteristics of a specific unit must be analyzed in detail in order to predict any indicators that may help the enemy. Size, activity, location, unit, time, and equipment, or SALUTE, are aspects of a unit that must be analyzed in order to determine any indicators a friendly unit may emit to the adversary. For example, a unit may be a small unit, but if the intent is to cause the enemy to think the unit is larger, specific actions would be required to make the unit appear larger to the adversary. Likewise, if we do not want an adversary to observe a particular unit entering a specific area of operations, we may change their uniform. Signature management must be taken into consideration during step one of the OPSEC process.

See appendix C for the process of determining unit-specific critical information.

Notes

- An extremely long critical information list (CIL) likely contains information that is not truly critical, and the list should be reworked. It is important to understand the difference between critical information and indicators that might be exploited to discover or deduce critical information.

- When an adversary knows of a vulnerability, it is no longer sensitive information, but should be looked upon as something to be minimized, eliminated, or coordinated with MILDEC.

3.4 STEP TWO: ANALYZE THREAT

Current, relevant threat information is critical in developing appropriate OPSEC protective measures. The threat assessment (TA) step in the OPSEC process includes identifying potential adversaries in the operational environment, and what their associated capabilities, limitations, and intentions to collect, analyze, and use knowledge of our critical information against us are. The threat refers to more than an enemy agent hiding behind a rock. There may be instances where there is no clearly defined threat; however, essential elements of U.S. military operations should still be safeguarded. The uncertain nature of the situation, coupled with the potential for rapid change, requires that OPSEC be an integral part of stability operations, both in a garrison and deployed environment. OPSEC planners must consider the effect of media coverage and the possibility such coverage may compromise essential security or disclose critical information. The following examples also represent threats:

1. An unauthorized person attempting to acquire critical information.

2. A person intentionally or inadvertently supplying critical information to an adversary.

3. A social media post mentioning details of a future deployment.

4. Someone overheard at, for example, the gym or education center talking about an upcoming deployment.

A threat is normally analyzed by determining who would want, and why they would need, specific information. Determining the value of a certain piece of critical information to an adversary will often help determine the lengths to which an adversary would go to acquire it. Various CI and intelligence organizations such as the Defense Intelligence Agency (DIA), Naval Criminal Investigative Service (NCIS), Federal Bureau of Investigation (FBI), or local law enforcement authorities can provide—in addition to organic resources—detailed information about an adversary's operational and intelligence collection capabilities, past, current, and projected, and the operational environment. (The role of the U.S. intelligence community and how they can assist in the OPSEC process is discussed in detail in chapter 7). OPSEC program managers, working with OPSEC survey personnel-assisted intelligence and CI staffs, answer the following questions:

1. Who is the adversary? (Who has the intent and capability to take action against the planned operation?)

2. What are the adversary's goals? (What does the adversary want to accomplish?)

3. What are the adversary's possible courses of action for opposing the planned operation?

4. What critical information does the adversary already have about the operations? (What information is too late or too costly, in terms of money or resources, to protect?)

5. What are the adversary's intelligence collection capabilities?

See appendix F for the process of determining and evaluating threat information relative to the OPSEC process.

3.5 STEP THREE: VULNERABILITY ANALYSIS

Indicators are those friendly actions and information that adversary intelligence efforts can potentially detect or obtain and then interpret to derive friendly critical information. An operation- or mission-related vulnerability exists when the adversary has the capability to collect indicators, correctly analyze them, and take timely action. Weaknesses that reveal critical information by means of collected and analyzed indicators create vulnerabilities. Vulnerability analysis identifies operation or mission vulnerabilities that an adversary could exploit to obtain critical information or indicators.

Note

> A vulnerability (i.e., a detectable, exploitable event) may or may not carry a security classification at the time of its identification; administrative or security controls, however, must still protect them disclosure.

To begin a vulnerability analysis, planners communicate with other security elements in the organization. Both OPSEC and traditional security programs seek to deny valuable information to adversaries by different yet complimentary approaches. Communications security plays a large role in OPSEC. COMSEC efforts can focus on specific communications' exploitation possibilities; our worst enemy may be a careless word. Cybersecurity also relates to OPSEC. Computer systems and networks are critical sources of sensitive information and require protection regardless of how their data is stored (DVDs, CDs, hard drives, flash drives, etc.). As a result, command COMSEC and cybersecurity planners provide quality input that can help identify existing vulnerabilities. Continuing to work with the intelligence and CI staffs, OPSEC personnel research the following questions:

1. What critical information indicators (friendly actions and open-source intelligence (OSINT)) will the planned operation generate through friendly activities?

2. Which indicators can the adversary actually collect?

3. Which indicators can the adversary use to the disadvantage of friendly forces? (Can the adversary analyze the information, make a decision, and take appropriate action in time to interfere with the planned operation?)

Based on the answers to these questions, personnel rank the criticality of the vulnerability. Vulnerabilities allow direct access to critical information, whereas indicators require some analysis to derive critical information. For example, when discussing important information over a nonsecure phone, vulnerabilities exist because the adversary may collect critical information directly. On the other hand, using a secure phone to discuss important information could be an indicator to the adversary that the organization is involved in something sensitive. Examples of indicators sometimes difficult to identify include:

1. Conducting work-related conversations in common areas or public places where people without a need to know are likely to overhear the discussion.

2. Increasing physical or administrative security around a particular project.

3. Requesting maps or information on particular geographical areas.

4. Applying for a passport or visa.

5. Making trip reservations.

6. Performing one's job the same way without considering what information may be gleaned from associated actions. In most cases, it probably does not make a difference, but what and how tasks are performed can be indicators.

See appendix F for the process of determining unit-specific vulnerability information.

3.6 STEP FOUR: RISK ASSESSMENT

Risk assessment, or measuring the level of risk, has two components. First, OPSEC program managers analyze the OPSEC vulnerabilities identified in the vulnerability analysis and identify possible OPSEC countermeasures for each. Secondly, OPSEC program managers, using risk assessment, select OPSEC countermeasures for execution; these are presented to the commanding officer and staff. OPSEC program managers, working with other planners and with the assistance of intelligence and CI organizations, provide risk assessments and recommend actions to mitigate vulnerabilities. Commanders then decide whether or not to employ the OPSEC measures. Risk assessments estimate an adversary's capability to exploit a vulnerability and the potential effects such exploitation has on operations. They also provide a cost-benefit analysis of possible methods to control the availability of critical information to the adversary. Effective OPSEC requires managing all dimensions of risk to maximize mission effectiveness and sustain readiness. Applying operational risk management enables avoiding unnecessary risks and accepting necessary risk when the cost of mitigation outweighs the benefit. To better assist an OPSEC program manager assess risk to a mission or activity, appendix G provides a risk analysis chart template along with an example of the risk assessment ratings criteria. Effective use of these tools greatly enhances a command's OPSEC posture.

See appendix C for the process of determining unit-specific critical information.

3.7 STEP FIVE: APPLY COUNTERMEASURES

OPSEC measures and countermeasures preserve military capabilities by preventing adversarial exploitation of critical information. Countermeasures mitigate or remove vulnerabilities that point to or divulge critical information. The management of the raw data controls critical information, increased potential for surprise enhances friendly force capabilities and augments the effectiveness of friendly military forces and weapons systems. OPSEC countermeasures fall under three general categories:

1. Prevent the adversary from detecting an indicator. A primary OPSEC goal is to mask or control friendly actions to prevent the collection of critical information or indicators. This includes using protective measures to create closed information systems, and using cryptographic protection and standardized security procedures. Communications security and cybersecurity are effective deterrents that prevent indicator detection. Another OPSEC tool that limits communications is River City. River City conditions provide procedures to control outgoing paths from ships and shore systems (e-mail, Web browsing, plain old telephone system, cell phones) for the purpose of OPSEC and force protection. Prior to commencing sensitive planning or operations that inadvertent communications or information release be could compromise, a River City condition should be considered with the following guidance. Implementation of River City requires commands to develop a prioritized information systems users list that identifies users by their need to access systems to perform mission-essential duties. The list should not be solely based on rank or pay grade, but based on function, and users placed into an appropriate group to support mission accomplishment. Those users who do not require access to systems to support mission planning or accomplishment should be grouped accordingly. (A complete list of River City conditions can be found in Navy-wide operation task IO.) Physical security may also become involved to thwart foreign human intelligence agents' access.

2. Provide alternative deceptive interpretations of an indicator. Sometimes controlling actions that reveal critical information or become the source of an OPSEC indicator may not be cost-effective. These circumstances may require attempts to disrupt or confuse the adversary's ability to properly interpret the information. Diversions, camouflage, concealment, and deception are methods that can be useful.

3. Attack the adversary's collection system. The third type of measure is to attack an adversary's intelligence collection system to eliminate or reduce their ability to obtain critical information. This category includes electronic warfare against technical collection platforms, and physical attack to destroy intelligence capabilities.

More than one countermeasure may be identified for each vulnerability. Conversely, a single countermeasure may be used for several different vulnerabilities. The most desirable OPSEC countermeasures combine the highest possible protection with the least impact on operational effectiveness.

OPSEC countermeasures usually entail some interference with normal operations, or a cost in time, resources, or personnel. If the cost to mission effectiveness exceeds the harm an adversary could inflict, the countermeasure is inappropriate. Because of the risk involved in not implementing a particular OPSEC countermeasure, this step requires command-level involvement.

Typical questions that might be asked during analysis include:

1. What is the potential risk to effectiveness if a particular OPSEC countermeasure is implemented?

2. What is the potential risk to a mission's success if an OPSEC countermeasure is not implemented?

3. What is the potential risk to a mission's success if an OPSEC countermeasure fails?

The interaction of OPSEC countermeasures must be analyzed. In some situations, certain OPSEC countermeasures may actually create indicators of critical information. For example, camouflaging previously unprotected facilities could indicate preparations for military action.

The selection of countermeasures may require coordination with other components or commands. Actions such as jamming intelligence nets or physically destroying the adversary's CI centers can be used as OPSEC measures. Conversely, deception and military information support operations plans may preclude applying OPSEC countermeasures to certain indicators in order to project a specific message to the adversary.

OPSEC Measures and Countermeasures should be measurable for performance and effectiveness.

3.7.1 OPSEC Measures

OPSEC measures are used to prevent adversaries from observing potential indicators or sources of critical information, but are not applied to specific vulnerabilities and threats. There are several OPSEC measures that are commonly employed:

1. Deception in support of operations security (DISO) is a military deception activity that protects friendly operations, personnel, programs, plans, capabilities, equipment, and other assets against adversary collection. The intent of DISO is to create multiple false indicators to confuse adversary intelligence gathering equipment or make friendly force intentions harder to interpret, limiting the ability of the adversary to collect accurate intelligence on friendly forces. DISO is general in nature. DISO is not specifically targeted against particular adversary decision-makers, but instead obfuscates friendly capabilities, intentions, or vulnerabilities, thereby protecting friendly operations and forces. OPSEC program managers must coordinate with their military deception (MILDEC) officer before planning or executing DISO.

2. River City is an OPSEC measure used to prevent the release of critical or sensitive information by controlling outgoing communications and network paths from a ship or location while allowing users to perform mission-essential duties. The operations cell of a command or activity makes the decision to set River City conditions. Communications personnel then limit access to all outgoing communications circuits and trunks such as Web traffic, e-mail, and phone lines. Any morale, welfare, and recreation networks must be shut down as well to prevent any communication outside the command. If implemented completely, only predesignated essential personnel have communication access in any form to the outside world.

3. Commands can use own-force monitoring to improve their OPSEC by monitoring the actions of their own force.

4. The National Security Agency's joint communications security monitoring activity (JCMA) supports DON commands by providing input of what the enemy is likely to perceive from monitoring friendly unencrypted communications or unclassified local area network (LAN) phone lines. JCMA provides joint COMSEC monitoring and analysis teams that support forward deployed units. Commands can request support from JCMA via their chain of command in accordance with OPNAVINST 2201.3B.

3.7.2 Application of Appropriate OPSEC Countermeasures

The command implements the selected OPSEC countermeasures or, in the case of planned future operations and activities, includes the countermeasures in specific OPSEC plans.

When executing OPSEC countermeasures, monitoring the adversary's reaction, if possible, can help determine countermeasure effectiveness and provide feedback. Planners use feedback to adjust ongoing activities and for future OPSEC planning. Coordination with intelligence and CI organizations ensures OPSEC requirements receive the appropriate priority.

INTENTIONALLY BLANK

CHAPTER 4

The OPSEC Assessment

4.1 SCOPE

The ultimate goal of OPSEC is increased mission effectiveness. To prevent our success, adversaries continually assess our capabilities and look for vulnerabilities to enact an asymmetric advantage. By preventing an adversary from determining friendly intentions or capabilities, OPSEC reduces adversary effectiveness, thereby increasing the likelihood of friendly mission success. Conducting regular OPSEC assessments enables mission success and demonstrates OPSEC's value. From hospitals to squadron commanders, supply depots to ships at sea, every unit that conducts an assessment immediately improves its mission effectiveness by implementing corrective measures to discovered vulnerabilities.

All naval commands shall conduct an annual internal OPSEC assessment to identify potential vulnerabilities and give the commander a holistic security assessment of operations, in accordance with OPNAVINST 3431.1A or MCO 3070.2A. An OPSEC assessment team examines an activity, process, or operation (mission) to determine if adequate protection from adversary intelligence exploitation exists. The team determines the relevant adversary intelligence or terrorist threat, identifies existing or potential problem areas, and recommends methods and procedures to improve the mission posture.

There are two types of OPSEC assessments: internal (conducted annually) and external (conducted triennially). This chapter focuses on the internal assessment; however, it also includes procedures for requesting external assessments.

OPSEC assessments are used to establish an indicator baseline for use in future assessments. An indicator baseline is developed to identify the basic operational characteristics of the force. This step includes assessing installed equipment as part of the force signature or profile that may be observable to interested parties. This information provides the foundation for overall OPSEC considerations. The IO staff updates and revises the baseline on a regular basis in order to ensure accuracy and relevancy with regard to the commander's intent and the operational environment. Whenever there is a significant change in operations (e.g., a new AO or a new mission), IO planners identify and evaluate the relative benefits and costs of maintaining or changing the baseline. Using the new baseline, IO planners update the assessment, revise the force operational profile, and provide additional support to other warfare area mission plans as necessary.

4.1.1 Enterprise Protection Risk Management

The operations security collaboration architecture (OSCAR) tool is embedded within the Air Force's Enterprise Protection Risk Management (EPRM) program. EPRM is a program that provides commands and commanders the ability to view enterprise-wide risk assessments across multiple functional areas in order to help make informed decisions on where to best allocate resources. OSCAR can be accessed and used via the EPRM program and is located on the SECRET Internet Protocol Router Network (SIPRNET).

4.1.2 The 14 OPSEC Assessment Benchmarks

Assessment of each unit's proficiency in accomplishing necessary OPSEC tasks under MCO 3070.2A, Secretary of the Navy instruction (SECNAVINST) 3070.2, and Department of Defense directive (DODD) 5205.02E have been divided into 14 functional areas referred to as benchmarks. They are:

1. Benchmark OPSEC-01: Program Implementation

2. Benchmark OPSEC-02: Analysis (Critical Information and Indicators)
3. Benchmark OPSEC-03: Analysis (Threat)
4. Benchmark OPSEC-04: Analysis (Vulnerability)
5. Benchmark OPSEC-05: Analysis (Risk)
6. Benchmark OPSEC-06: OPSEC Measures
7. Benchmark OPSEC-07: OPSEC Working Group
8. Benchmark OPSEC-08: Training and Awareness
9. Benchmark OPSEC-09: OPSEC Review
10. Benchmark OPSEC-10: Coordination
11. Benchmark OPSEC-11: Contracting and Contracts
12. Benchmark OPSEC-12: Subordinate Units
13. Benchmark OPSEC-13: Annual Report
14. Benchmark OPSEC-14: Resources

The Marine Operations Security Support Team (MOST) developed and now employs benchmarks in order to evaluate the OPSEC posture of a Marine Corps unit.

Program management includes all associated tasks with benchmark OPSEC-01, program implementation. This benchmark assesses the organization’s compliance with OPSEC program implementation and program management in accordance with MCO 3070.2A, and evaluates the following:

1. Has the unit OPSEC manager or coordinator been appointed in writing?
2. Does the OPSEC manager possess the requisite security clearance to perform their duties?
3. Has the unit published an OPSEC policy or standard operating procedure (SOP)?
4. Is OPSEC integrated into the installation or organization’s planning and operations?
5. Is there an OPSEC tab included in each unit’s operations order?
6. Are internal OPSEC assessments being conducted?
7. Does the OPSEC program manager or coordinator maintain a current continuity binder?
8. Is the unit’s OPSEC program assessed for effectiveness at least annually?
9. Does the organization have an OPSEC support capability that provides for program development, training, assessments, surveys, and readiness training?

Benchmarks OPSEC-02 through OPSEC-06 evaluate the foundation of the unit’s compliance with the standardized Department of Defense (DOD) five-step OPSEC process. These benchmarks are:

1. Benchmark OPSEC-02: Analysis (Critical Information and Indicators) (Phase One)
2. Benchmark OPSEC-03: Analysis (Threat) (Phase Two)

3. Benchmark OPSEC-04: Analysis (Vulnerability) (Phase Three)
4. Benchmark OPSEC-05: Analysis (Risk) (Phase Four)
5. Benchmark OPSEC-06: OPSEC Measures (Phase Five)

These five benchmarks assesses the unit or organization's performance of the DOD's OPSEC process that begins with understanding and determining that which the unit commander deems to be critical information. Afterwards, it is essential to understand the threats and vulnerabilities associated with this critical information, and the risks, including acceptable levels of risk in losing critical information to compromise or adversarial collection. Finally, benchmark OPSEC-06 evaluates whether the unit has identified and successfully implemented OPSEC measures to minimize compromise, and plans to mitigate vulnerabilities associated with the unit's critical and sensitive information.

Benchmarks OPSEC-07 through OPSEC-14 assess the organization's accomplishment of OPSEC tasks associated with a successful OPSEC program. These benchmarks are:

1. Benchmark OPSEC-07: OPSEC Working Group
2. Benchmark OPSEC-08: Training and Awareness
3. Benchmark OPSEC-09: OPSEC Review
4. Benchmark OPSEC-10: Coordination
5. Benchmark OPSEC-11: Contracting and Contracts
6. Benchmark OPSEC-12: Subordinate Units
7. Benchmark OPSEC-13: Annual Report
8. Benchmark OPSEC-14: Resources

These 14 benchmarks are clarified further in appendix P.

4.2 INTERNAL OPSEC ASSESSMENT

The internal OPSEC assessment, which is conducted annually, is a process that evaluates an operation, activity, exercise, organization, or support function, and determines the likelihood that commands can protect critical information from the adversary's intelligence collection capabilities. The general methodology of an OPSEC assessment applies to all commands, but specific procedures vary depending on a mission's focus. An effective assessment requires cooperation and participation from all hands. Since team or working group members may question individuals, observe activities, and gather data during the course of the assessment, the commander should inform all hands in advance. The command should emphasize that while the assessment is not an inspection, it improves mission effectiveness and performance through identification and elimination of potential vulnerabilities that may impact mission accomplishment.

OPSEC within naval forces is primarily concerned with protecting mission accomplishment from hostile intelligence, terrorist, or hacker exploitation. The internal OPSEC assessment completes the identification of exploitable sources of information.

An internal OPSEC assessment uses a command's own personnel and resources to conduct an examination of the command's processes and methodologies with the ultimate goal of increasing mission accomplishment. Appendix H provides a list of recommended members and responsibilities.

Every OPSEC assessment is unique. Assessments differ based on the nature of the information, adversary collection capability, and environment of the activity. Emphasis must be focused on identifying mission-related indicators that signal friendly intentions, capabilities, and limitations that permit the adversary to counter or reduce the effectiveness of friendly operations. In peacetime, assessments generally seek to correct weaknesses that disclose information useful to potential adversaries in the event of future conflict. Many activities, such as operational unit tests and major exercises, interest a potential adversary because they provide insight into friendly readiness, plans, crisis procedures, infrastructure support, and command and control procedures and capabilities.

Careful planning, thorough data collection, and thoughtful analysis are keys to an effective internal OPSEC assessment. A successful assessment requires a team with expertise in the functional areas being examined, as well as team members who bring an unbiased examination approach.

The internal OPSEC assessment identifies what an adversary might perceive and identify as potential information sources. The assessment represents a data gathering effort that differs from a hostile country's effort in that it uses minimal manpower, has a limited time frame, and does not use deception. The internal assessment identifies potentially exploitable information sources and verifies the indicators disclosed by examining all functions taking place during planning, coordination, and execution of operations, or any activity undergoing evaluation.

Internal OPSEC assessments focus on a specific operation, process, or activity. Though missions and functions of different commands vary, there are certain procedural similarities for conducting an assessment that can be divided into three phases: planning, assessment and analysis, and reporting.

4.3 INTERNAL OPSEC ASSESSMENT PROCEDURES

Conducting an effective internal OPSEC assessment requires planning and sufficient time for a thorough review of pertinent documentation, formal and informal coordination and discussions, and preparation of a task plan of the mission/activity. Key members of the internal OPSEC assessment team meet in the planning phase.

4.3.1 Planning Actions

1. Preparations for an internal OPSEC assessment begin well in advance; the required lead-time depends on the nature and complexity of the operation and activities to be assessed (e.g., combat operations, peacetime operations, etc.). The planning phase should include sufficient time for a thorough review of pertinent processes and documentation, formal and informal coordination, and discussions.

   a. Program managers identify which of the command's activities, projects, processes, programs, or missions to consider—from only one to all of the organization's operations.

   b. Program managers then determine which work unit, including associated support and management, use the information with sensitivity in question. Additional work units can be added to the list during the assessment.

2. The second step of the process is to select the OPSEC assessment team members. Additional details on the composition and responsibilities of the OPSEC assessment team are in appendix H.

   a. The team should include multidisciplinary expertise. Assessment team members require analytical, observational, and problem-solving abilities.

   b. The latitude of the assessment serves as a guide to select assessment members. As practical, program managers assign previous OPSEC assessment team members to maintain a high level of continuity.

   c. Since assessments are normally oriented toward operations, the senior member should be from the operations staff of the commander responsible for conducting the assessment.

d. Other team members represent the functional areas of intelligence, security, communications, logistics, plans, and administration. As strike groups are deploying with coalition forces with increasing frequency, the foreign disclosure officer should also be an integral member of the team. When appropriate, specialists from other functional areas such as transportation and public affairs may participate.

e. When communications monitoring is part of the assessment, the monitoring group leader should be a member of the OPSEC assessment team. Team members meet early in the planning phase to ensure timely, thorough accomplishment of the tasks outlined below.

3. All team members should become familiar with assessment procedures and techniques, especially when team members do not have previous assessment experience.

4. The team members' understanding of the operation or activity to be assessed is crucial to ensuring the success of phases of the assessment. Team members should become familiar with the operation plans, orders, standard operating procedures, associated processes, or other directives bearing on the assessed operation or activity. This initial review familiarizes team members with the mission and concept of operation and identifies most of the organizations participating in the assessed activity; others may be identified as the assessment progresses.

5. Members develop or verify the current critical information list for the mission, and hold a dialogue on how to determine critical information, including the process used to identify what to consider critical. This may include a discussion of information developed through open sources, official threat studies, and information elicited from mission personnel. Identification of critical information is paramount to a successful assessment. Program managers ensure that all parties—the assessed and the assessors—agree on the developed critical information. Program managers review and validate critical information throughout the assessment, to include the briefing process, as well as after completion of the assessment in order to ensure that everyone agrees on what constitutes critical information.

6. Team members develop a threat assessment statement by identifying adversaries, their goals, and objectives. Each operation may have several adversaries whose goals are in conflict with friendlies or one another. To fully identify an operation's adversaries, the OPSEC program manager and assessment team need to know of any potential adversary entity's intentions. Because intentions, in most instances, are known only through capabilities, program managers require detailed information to understand and analyze capabilities into these intentions.

7. It is necessary to determine EEFI in order to develop a critical information list (see chapter 3).

8. It is also necessary to determine sources of information, i.e., where an adversary may obtain critical information.

9. During the initial review, team members begin to develop functional outlines for respective areas of interest. The team needs to know who, what, how, when, where, and why significant events occur during the assessment period. Command profiles are basic guides for this step. Collectively, command profiles or functional outlines project a visual picture of an operation. The events to be observed at various levels should be related to the appropriate organizational element in order to allow observation at those locations during the assessment phase.

10. Planners announce the strategy for the assessment to the command, including:

    a. Purpose and scope

    b. Team members and their clearances

    c. Required briefings and orientations

d. Time frame

e. Administrative support requirements

f. COMSEC, cybersecurity, and automated information system (AIS) monitoring requirements, if applicable.

11. The OPSEC team interviews command individuals to gain insight into daily processes and procedures. The OPSEC working group develops of standard questions in order to evaluate each person's awareness of OPSEC, its application, and the relevant threat. If interviewing 100 percent of the command is impractical, the team ensures the interviewing of a representative sampling of each department or division.

4.3.2 Internal OPSEC Assessment Analysis

During this phase, the OPSEC team correlates the data that individual members acquired. The team compares notes, assimilates data, and analyzes the operations, intelligence aspects of the operation, and communications, if applicable. Tentative conclusions may be validated or disproved through introduction of changes into suspected operational patterns. If evidence of foreign knowledge correlates to friendly action or actions prior to or during operations, make a determination as to whether or not these correlations continue after introducing changes. In the final analysis, positive or highly suspect sources of information that are subject to hostile exploitation should be identified and supported in detail.

4.3.3 Identification of Vulnerabilities

Correlation and analysis of data helps the team to refine the previously identified vulnerabilities or isolate new ones. Indicators that are potentially observable are identified as vulnerabilities. Vulnerabilities point out situations that an adversary may be able to exploit. The key elements of vulnerabilities are observable indicators and an intelligence collection threat to those indicators. The degree of risk to a friendly mission depends on the adversary's ability to react to a given situation in sufficient time to degrade friendly mission or task effectiveness.

4.3.4 Internal OPSEC Assessment Reporting

Internal OPSEC assessment reports do not have a specific format. The report should create a discussion of identified critical information, indicators, and an adversary's intelligence capabilities, OPSEC vulnerabilities and, ultimately, recommend OPSEC measures to eliminate or reduce the vulnerabilities. Although some vulnerabilities may be virtually impossible to eliminate or reduce, program managers should include them in the report to enable the commander to more realistically assess the operation or activity. The OPSEC program manager tracks the findings until corrected. Many commands use a PowerPoint presentation for in-brief, out-brief, and plan of action and milestones. Assessment findings are kept within the command's chain of command. The command maintains results for three years.

4.4 EXTERNAL OPSEC ASSESSMENTS

An external assessment requires a team comprised of subject matter experts from multiple disciplines from outside the command or unit in order to simulate adversary intelligence processes. An external assessment should focus on the organization's ability to adequately protect critical information from adversary intelligence exploitation during planning, preparation, execution, and post-execution phases of any operation or program. These assessments may include telecommunications monitoring, radio frequency monitoring, network and computer systems assessment, and open-source collection. External assessment teams should use collection techniques of known adversaries. This type of assessment is required triennially. See figure 4-1 for an internal-external assessment comparison.

Internal and External Assessment Comparison	
Operations Security Internal Assessment	**Operations Security External Assessment**
Purpose: To determine the likelihood that critical information can be protected based on procedures currently in place.	Purpose: To reproduce adversary collection capabilities against an organization to determine if critical information may be disclosed through normal operations and functions, to identify vulnerabilities, and to propose countermeasures.
Scale: Small in scale. Focused on evaluating operations security program effectiveness.	Scale: Large in scale. Focused on analysis of risks associated with an operation or organization's mission.
Frequency: Annually.	Frequency: Triennially or when operations or commanders dictate.
Resources: Internal resources (e.g., security, public affairs, communications personnel) are used to conduct the assessment.	Resources: External resources (e.g., operations security support elements, communications security monitors, red teams) are collectively used to conduct the survey with or without the use of indigenous resources.
Design: Internal OPSEC assessment should include a planning, execution, and analysis phase. Minimal planning is required to conduct an assessment. A briefing or executive summary may be used to present findings.	Design: External OPSEC assessment planning is extensive and should include a planning, preparation, execution, and post-execution phase. A comprehensive report is generated.

Figure 4-1. Internal and External Assessment Comparison

DODM 5205.02-M requires external OPSEC assessments be conducted every three years. Afloat and ashore commands may submit requests for external OPSEC assessments to their respective OPSEC support element via their ISIC. The Naval Operations Security Support Team (NOST) located at Navy Information Operations Command Norfolk is the Navy's OPSEC support element chartered to perform external OPSEC assessments. The Interagency Operations Security Support Staff (IOSS), Joint Information Operations Warfare Center's Joint OPSEC Support Center, and Army's 1st Information Operations Command (Land) OPSEC support element are also chartered organizations to perform external assessments. U.S. Marine Corps units can submit requests for external OPSEC assessment help via the chain of command to either the NOST or Marine Corps Information Operations Center OPSEC support element.

Due to the intense resource requirements to conduct triennial external assessments, the ISIC should be request, drive, and support them.

4.5 EXTERNAL RESOURCES

Depending on the scope of the internal OPSEC assessment, commands may not possess the requisite expertise to collect or analyze data. External resources can provide subject matter expertise.

4.5.1 Communications Security

Communications security is the protection resulting from all measures designed to deny unauthorized persons information of value that could 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. Navy commands desiring COMSEC monitoring support can submit a request in accordance with guidance contained in NTISSD 600 (COMSEC Monitoring) and OPNAVINST 2201.3 (COMSEC Monitoring of Navy and Marine Corps Telecommunications and AIS). COMSEC support provides an analysis of the communications profile of a site.

4.5.2 Human Intelligence

Human intelligence (HUMINT) is derived from information collected and provided by human sources. An assessment of the HUMINT threat for a particular area should begin with reviewing intelligence reports of the area involved. A current list of threat briefings can be found on the SIPRNET NCIS homepage (https://www.ncis.navy.smil.mil/).

4.5.3 Fleet Defensive Cyberspace Operations

Fleet Defensive Cyberspace Operations, defensive cyberspace operations (DCO), or Blue Team personnel conduct a series of procedures to determine whether vulnerabilities exist in a ship's AIS infrastructure. Blue Team assessments are scheduled every two years, or when network infrastructures are changed. Detailed procedures on DCO are located in Navy information operations command (NIOC) TACMEMO 3-12.1-17, Defensive Cyberspace Operations Tactics for Surface Forces. The publication can be accessed on SIPRNET at https://www.portal.nwdc.navy.smil.mil/NDLS/pubs/forms/TACMEMOS.aspx. Requests for these services are sent via unclassified message to NIOC Norfolk (with passing instructions to N3). The Marine Corps Cyberspace Operations Group supports U.S. Marine Corps units, and units operating on the Marine Corps Enterprise Network with DCO capabilities. To request DCO support from the Marine Corps Cyberspace Operations Group, submit a naval message to Marine Forces Cyber Command detailing the support requested.

4.6 ASSESSMENTS DURING THE OPTIMIZED FLEET RESPONSE PLAN

OPSEC is a critical and key program in protecting information, especially during deployments, testing of new equipment and capabilities, and during a ship's training cycle or optimized fleet response plan (OFRP). Every unit in the training cycle and scheduled for deployment, whether as part of a strike group or independent deployer, should have a functioning OPSEC program. The best method in determining a unit's OPSEC program and overall posture is through the completion of a required self-assessment. This chapter discusses the roles and responsibilities of the NOST during the OFRP cycle.

4.6.1 Considerations

During the OFRP, the NOST can assist with the following:

1. Ensure OPSEC program managers and coordinators are provided the opportunity to attend the Navy OPSEC program manager course (J-2G-0966). Courses are regularly scheduled on each coast and fleet-concentrated areas. The NOST accommodates program managers and coordinators to the maximum extent possible based on ships' schedules.

2. Schedule and conduct an assist visit with the unit's OPSEC program manager. The initial visit determines the status of the unit's OPSEC program, and provides the program manager with the necessary tools to establish or improve their program. This includes training on conducting a unit OPSEC assessment. Before departing the unit, a return visit should be coordinated and agreed upon.

3. Validate and review the unit's self-assessment. This should be completed 30 to 45 days after the initial assist visit. NOST members provide immediate feedback and recommendations for improvement (if any) on the unit's overall program.

4. Provide written report to the program manager and ISIC.

4.6.2 Purpose

The NOST assesses a unit's OPSEC program during the OFRP cycle to ensure the unit is prepared for deployment. Not only is OPSEC required, but when included in the OFRP, it provides the unit's commander and information operations warfare commander a better understanding of the strike group's or readiness group's OPSEC posture. Figure 4-2 depicts OPSEC in the OFRP cycle.

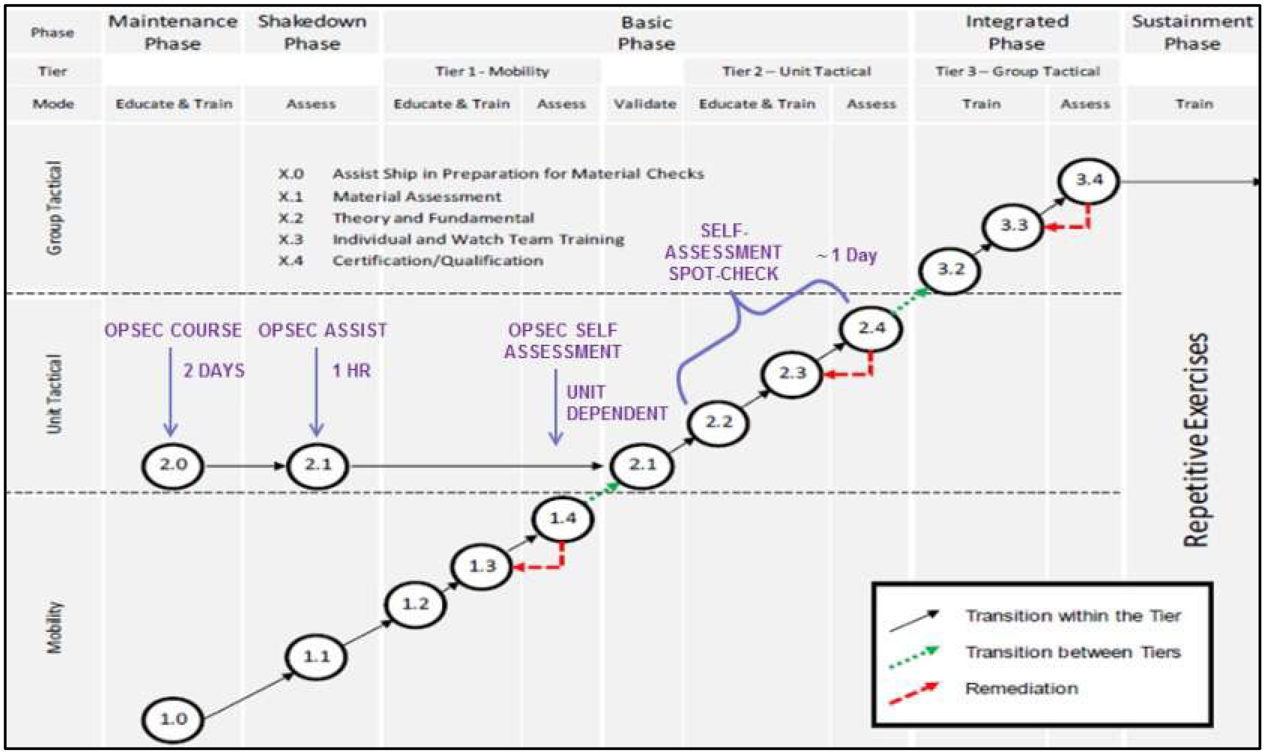


Figure 4-2. Internal Optimized Fleet Response Plan Cycle

INTENTIONALLY BLANK

CHAPTER 5

OPSEC’s Role in Operational Messages

5.1 SCOPE

Commands should give OPSEC key consideration when releasing operational messages or while using e-mail or chat in an official capacity. Judiciously using OPSEC reduces the risk of compromising sensitive unclassified information in a variety of messages and e-mails ranging from protocol to medical support requests. Applying the OPSEC process denies plan details, practices, and capabilities to potential enemies and others without a need to know. This chapter addresses the logistics requirement (LOGREQ), one of the most common shipboard operational messages, and provides guidance for safeguarding potentially sensitive but unclassified information. Other operational messages (e.g., Operational Report-3 Navy Blue, Pinnacles, or Unit Situation) may result in some observable change within a command, but are governed by a separate set of instructions not addressed in this publication. Any actions resulting from an operational report message require OPSEC considerations.

5.2 LOGISTICS REQUEST

This LOGREQ guidance balances force protection (FP) and OPSEC requirements, while maximizing host nation (HN) and husbanding contractor flexibility in arranging logistics support for units. OPSEC’s very situational nature enables applying similar procedures to other routine evolutions (e.g., mail routing instructions, and morale, welfare, and recreational events).

In view of the continued importance of FP, it is critical that action be taken to minimize unnecessary dissemination of port visit information. Planners should consider the following recommendations:

1. LOGREQ information becomes unclassified (UNCLAS) once diplomatic clearance is released to the HN. In continental United States (CONUS) ports and in ports where diplomatic clearance is not required due to standing agreements, the UNCLAS LOGREQ message does not contain the date of ship arrival and the FP LOGREQ is not used to specify the time of ship’s arrival.

2. The diplomatic clearance request and FP LOGREQ messages are normally classified at least Confidential—Releasable to the HN. In instances where a single LOGREQ is submitted, including FP LOGREQ data, the LOGREQ is classified at least Confidential—Releasable to the HN.

3. There are two methods of passing logistics requirements: a combined ship and FP LOGREQ after release of diplomatic clearance to the HN, or an initial LOGREQ followed by supplemental LOGREQ and FP LOGREQ messages. UNCLAS LOGREQs submitted before release of diplomatic clearance to the HN do not contain the date of ship arrival.

4. When used, UNCLAS LOGREQ and FP LOGREQ messages are transmitted immediately after ship or unit release of the diplomatic clearance request message to facilitate adequate logistic support.

5. The specific date combined with the specific time of ship arrival is considered sensitive and therefore shall not be included together in UNCLAS LOGREQ messages. In most circumstances, the diplomatic clearance request and UNCLAS LOGREQ contain port visit dates and the FP LOGREQ is used to specify time of ship’s arrival. Message supplements are used should date or time change. Specific submarine arrival time may be withheld from disclosure to husbanding contractors up to 48 hours prior to arrival as operational requirements and policy deem necessary.

6. Ships and submarines include the servicing fleet logistics center (FLC) or Military Sealift Command as applicable and Naval Supply Systems Command Global Logistics Support on the FP LOGREQ to facilitate husbanding services planning and contracting.

7. To raise awareness that even unclassified port visit information is sensitive, the following statement shall be included at the beginning of paragraph one in the LOGREQ: “Information concerning U.S. ships’ operations, movements, and activities are potentially sensitive and shall be passed only to the individuals who must know it in the performance of their duties. Only the minimum required information should be shared.”

8. Regarding logistics requirements, the contracting officer (KO) should pass the ship’s schedule information to husbanding services contractors. Prior to diplomatic clearance release to HN, KOs should limit information given to potential husbanding services contractors to hull type (not specific name of the ship) and duration (not date-specific) of port visit. Once the defense attaché office (DAO) or embassy receives diplomatic clearance approval and release to HN, KOs are authorized to provide husbanding contractors the name of the ship, date, and time of arrival from the diplomatic clearance or FP LOGREQ supplement.

9. KOs are responsible for all communications and ordering of goods and services with the husbanding contractor. This is particularly critical in ports without a nearby U.S. Navy support activity where substantial coordination is required. Regarding name of the ship, date, and time of arrival, it should be stressed to each contractor or person that disclosure of these three pieces of information together (unit name, date, and time of arrival) is sensitive information, and should not be divulged to subcontractors to the maximum extent possible without impacting adequate husbanding services provision.

10. When passing a ship’s arrival information over nonsecure circuits, including UNCLAS e-mail, refer to the LOGREQ by message date and time group, and refer to data fields by line number. When discussing a specific ship’s LOGREQ, do not associate the ship’s name, side number, or any other distinguishing characteristics with the information in the LOGREQ.

KOs ensure husbanding contractors understand it is imperative that contractors understand the privileged nature of ship movement information, and that they are strongly discouraged from simultaneously discussing a ship’s name, time and date, or arrival in conversation when using the phone or e-mail. Although the Navy Security Manual or other guidance may deem information unclassified, dissemination of ship’s port visit information should be controlled to the maximum extent possible. The husbanding contractor requires elements of this information. However, every effort should be made to minimize disclosure of sensitive information, specifically the unit name, date, and time of arrival. Commands sending advance parties should coordinate directly with the DAO and the U.S. embassy to obtain approval and ensure the servicing FLC KO is apprised of any logistics requirements.

5.3 CONCLUSION

The above listed measures are not all-inclusive. Ultimately, common sense should prevail when drafting messages or sending e-mail or chat sessions that contain potentially sensitive information. If sensitive information must be transmitted via nonsecure means, every effort should be made to minimize the amount of information put at risk.

CHAPTER 6

Web Risk Assessment and Web Site Registration

6.1 SCOPE

Chapter 6 discusses the proliferation of publicly accessible information found on the Internet and the need for prudent OPSEC measures. Application of the OPSEC five-step process is imperative when placing information on the Internet. Web site self-assessments are a useful tool in determining whether potential critical information is on a command's Web site. Appendix K provides a self-assessment checklist. Information regarding online surveys, and guidance for requesting Web risk assessments and written guidance for Web site registration are provided in section 6.6.

6.2 OVERVIEW

Given the increasing dependence of our national and economic security upon the information infrastructure, it is essential that the commander and other organizational heads review information connectivity and content to ensure good OPSEC procedures within their organizations. As such, risk assessment and risk management become critical factors in evaluating Web site information. Anything posted to the Internet is available to any adversary. Adversary intelligence collection threats include the exploitation of publicly available information often obtained through open networks and information on websites. These and other detectable activities are used to derive indicators of U.S. intentions, capabilities, operations, and activities. A necessary condition for maintaining essential secrecy is protection of classified, as well as unclassified critical information.

The worldwide connection of local area networks and wide area networks such as the Nonsecure Internet Protocol Router Network (NIPRNET) make access to DOD information from anywhere in the world relatively easy. Separation between the NIPRNET and the Internet is ambiguous, and occasionally these networks may be indistinguishable to Web page administrators. Web pages intended for internal DOD use should not be made available on the NIPRNET without appropriate access control, as this information is likely to be accessible to non-DOD users. Consequently, OPSEC and information security (INFOSEC) concerns arise. This requires a convergence of INFOSEC tools and the OPSEC process at the activity level. Activity Webmasters, page maintainers, subject matter experts, and OPSEC personnel must develop a disciplined review of all information posted to their locally generated Web sites. This must be done to protect sensitive unclassified information—while recognizing the importance of making available timely and accurate information to the intended DOD audiences, the public, Congress, and the news media.

Evaluations of activity information provided on the NIPRNET and publicly accessible DOD Web sites on the Internet should follow this OPSEC methodology:

1. Identify information access points (NIPRNET, Internet, etc.) and evaluate their importance to activity operations.

2. Determine the critical information for the activity's operations and plans.

3. Determine the threat—assume that any potential adversary has access and knows how to search the Internet.

4. Determine the vulnerabilities—how protected are the Web pages?

5. Assess the risk—what protection should be applied to minimize potential loss of critical information, and what is the impact on operations and operations support?

6. Apply protection—minimize information loss and vulnerability.

When applying the OPSEC process to information posted to Web sites, evaluate the data with regard to the time factor. Information gathering in the past was a manpower- and resource-intensive process that depended on various types of overt and clandestine means. Collection, compilation, analysis, and dissemination of information could take days, weeks, or months. Today, a single user can connect to the Internet and, using various search engines, browsers, and aggregation methods, can develop a composite of information that surpasses traditional knowledge levels. In essence, geography is no longer a factor in information retrieval—time becomes the dominant factor.

The user must determine the value of information with regard to time. Certain data, (unit history, emblems, command affiliation, etc.) has less time criticality than do deployment orders for exercises or real-world operations. The value of information may also flex over time. For example, the specifics of predeployment preparations should not be posted to a publicly accessible Web site prior to the deployment. But once in theater, unit types, number of personnel, and equipment becomes public knowledge over time, decreasing the sensitivity of the data. Subsequently, the same information again becomes sensitive as redeployment dates and unit withdrawal specifics are planned. This requires units to actively scrub their Web pages for time-sensitive data. Even after removal, information may still be retrievable. Information removal is recorded and available through sites such as: https://archive.org/web.

6.3 OPSEC AND THE INTERNET

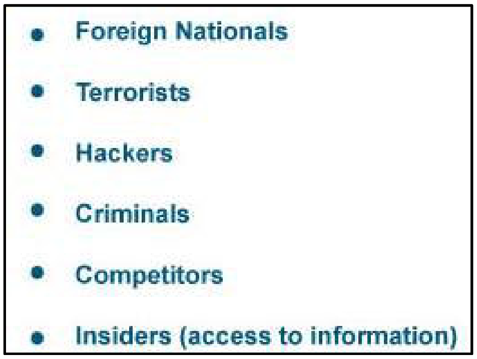
OPSEC program managers should review their command's Web site through the eyes of the adversary, looking for critical information that could reveal sensitive operations, movement of certain assets, personal information about U.S. citizens and employees, and technological data.

The worldwide public, including the American taxpayer and media, may view and interpret information residing on a server with a ".mil" domain. There is no such thing as a personal or unofficial Web page on a .mil server. These servers and the information they contain shall be used only for official business and in an official capacity. Publicly available information does not include classified material, information that is sensitive, or information that could enable the recipient to infer classified information.

Only information of value to the general public that does not require additional protection should be posted to publicly accessible sites on the Internet. Information requiring additional protection, such as controlled unclassified information (CUI), information not specifically cleared and approved for public release, or information of questionable value to the general public and for worldwide dissemination poses an unacceptable risk to the DOD, including military personnel and civilian employees, and should either not be posted at all or placed on Web sites with security and access controls. Appendix O contains a risk decision flow chart on posting information on the Internet.

It is not necessary for our adversaries to spend much time gathering information about our missions or the activities of our personnel if that information is provided to them on the organization's or command's official Web site, or by means of DOD employee's or contractor's private Web site (see figure 6-1). While the Internet provides a powerful tool for conveying information quickly and efficiently to conduct daily activities, it also increases the risk and threat to the organization and its employees. Today's technology poses a particular problem in that Internet connectivity provides a singular user with new and increasingly efficient tools for reviewing and compiling information.

Today's data-mining capabilities enable individuals to quickly collect small pieces of information from any number of different sources and quickly compile them into a product that contains sensitive, and very possibly, classified information. Geography is no longer a factor in information gathering, or to select and develop knowledge about a target.



- Foreign Nationals
- Terrorists
- Hackers
- Criminals
- Competitors
- Insiders (access to information)

Figure 6-1. Adversaries on the Web

For OPSEC program managers, this means that information posted on Web sites may pose more risk than information about the organization and its mission that is available through other means. Using information on one Web site, an analyst can quickly search the Internet for other sites that expound upon that information, and then derive indicators that point to or ascertain the critical piece of information necessary to thwart the command’s mission. Using conventional information-gathering techniques, it could take days or even weeks to gather such information whereas on the Internet, only hours—or even minutes.

Because of the increased risk that someone may piece together the information puzzle, small items of information posted on publicly accessible Web sites are of increased OPSEC significance. An OPSEC program manager can no longer simply review the activity’s Web site for items that may be targets for an adversary, since there is no way of specifically identifying which items in conjunction with information from other sites or sources may become critical indicators.

OPSEC program managers should caution employees on what should or should not be posted on their own personal Web sites and DON publicly accessible Web sites. Contracts can and should contain OPSEC restrictions wherein the activity reviews and approves information prior to posting on the contractor’s Web site, in order to minimize inadvertent disclosure of critical information.

An OPSEC solution to this apparent security dilemma is to adopt a zero-based approach to Web site content. Decide which items combined with other information would be critical to an outside collector. Use OPSEC procedures to determine what information is absolutely necessary to post on Web sites to fulfill the mission and do not post any other information. Below are the most important considerations in zero-based Web site security:

1. Assess the benefits to be gained by posting specific types of information on a Web site. Identify a target audience for each type of information and why their need for the information is important to the organization’s mission. A careful examination of the potential consequences of placing information on the Web site is necessary.

2. Post only information for which the activity is responsible. Since an organization knows its own critical information best, it can reduce the vulnerability of other organizations by letting them post their own information.

3. Do not post public links to more sensitive sites. These links identify the existence and location of potential targets for a collector who may have previously been unaware of them. If it is necessary to link to other sites, the link should pass through an intermediate site that can screen visitors through passwords or other criteria.

In the past, OPSEC focused on activities that a human observer, a satellite, a radio intercept operator, or the news may not have seen or showed. With the proliferation of information technologies over the last three decades, however, the access to DOD data has grown exponentially. The old threats have not gone away, but there is a new area of concern that OPSEC program managers and planners must consider—the Internet. A disciplined approach to the OPSEC process ensures that sensitive information is properly protected.

6.4 POSTING PICTURES ON THE INTERNET

Pictures must be carefully scrutinized prior to posting on the Internet. Pictures can carry exceptional weight for intelligence collectors. They allow an intelligence collector to conduct surveillance from the safety of a computer without ever having to set foot near the objective. Aerial photographs of facilities, detailed photos of a certain aspect of a facility, and pictures of equipment may all be used and pieced together to form a full-sized portrait. When deciding whether or not to release a photo on the Internet, be sure to look at what is in the background. Consider what we would not want our adversaries to have access to, such as security features, equipment that may be of particular value to foreign competitors, or badges and other items unique to individual operations and activities.

Commands must also consider the risks when posting pictures and information about command members. Highlighting individuals for a job well done is an excellent way to project the Navy's image and individual accomplishments, but may also put them and their families at risk if too much information is released. SECNAVINST 5720.44C provides guidance on releasing personal information to the public.

Intelligence collectors are known to target and elicit information from Navy members and their families. We carry advertisements on us every day that indicate for whom we work: uniforms, parking passes, DOD decals, badges, organizational T-shirts, and stickers. When we add these indicators to information available on the Internet, our exposure increases exponentially.

6.5 WEB RISK ASSESSMENTS AND REVIEWS

The Web Risk Assessment Cell located at Navy Network Warfare Command (NETWARCOM) conducts two types of Web risk assessments on all DON Web sites annually. The first is a technical vulnerability scan, conducted remotely from NETWARCOM using various software scanning tools, and it attempts to identify Structured Query Language injections, cross-site scripting, and other well-known vulnerabilities. Results are posted to the Defense Information Systems Agency-hosted Web Vulnerability Scanning portal on SIPRNET, and are reported to Navy Cyber Defense Operations Command. The Navy Cyber Defense Operations Command contacts the site if any mitigation is required. The second assessment is an annual Web site compliance and content review that ensures all Web sites meet DOD and Navy policy as well as posting only releasable information (DOD consent banner, correct privacy act statement, links to appropriate organizations, etc.). The command requires that self-assessment reviews are performed using a check sheet that the WRA Cell at NETWARCOM provides. Content or OPSEC reviews of Web sites also reside with the Web site owner because of the command's familiarity of the mission and critical information.

6.6 WEB SITE REGISTRATION

A Web site self-assessment must be completed before a site goes on-line. The Webmaster is then responsible for registering the site with NETWARCOM. The Webmaster also has responsibility for reregistering the site annually, or when significant information changes, whichever occurs first. Defense Media Activity Marines must vet and approve all Marine Corps Web sites and Web presences. All vetted and approved sites and presences must then be registered with U.S. Marine Corps office Web site. More information on the Marine Corps Web site registration process is found at http://www.marines.mil/Units/SiteRegistration.aspx.

CHAPTER 7

Naval Criminal Investigative Service Contributions to the OPSEC Process

7.1 SCOPE

This chapter provides an overview of the U.S. intelligence community and how information it provides can assist the commander when implementing the OPSEC process and making decisions.

7.2 OVERVIEW

OPSEC program managers should always attempt to get threat intelligence from their command's intelligence officer first. If that resource is not available, program managers can look to other sources of intelligence. NCIS is the primary source of intelligence on asymmetric threats (e.g., terrorism, foreign intelligence, criminal, cyber, etc.) to DON activities. NCIS maintains and operates a worldwide Federal law enforcement organization to fulfill the investigative and CI needs of the United States Navy and Marine Corps. NCIS ensures that the commands it supports have the most accurate and relevant intelligence information needed to protect themselves from threats of terrorism and sabotage, criminal and cyber threats, and foreign intelligence collection.

NCIS is also the executive CI agent to several Department of Defense agencies, including the Defense Finance and Accounting Service and the Defense Advanced Research Projects Agency. NCIS also provides CI support to combatant commanders through the command CI coordinating authority, CI support officers assigned to the unified commands (such as USPACOM and the Joint Staff), and CI specialists assigned to joint analysis centers and various joint intelligence centers.

NCIS provides antiterrorism/force protection (AT/FP) support and services to the U.S. Navy and Marine Corps from over 150 worldwide field locations. In addition to organic intelligence assets, NCIS provides invaluable data for making OPSEC considerations for a variety of evolutions. NCIS mission priorities are as follows:

1. Prevent terrorism and other hostile attacks against DON forces and installations

2. Protect against compromise of DON sensitive information and critical systems

3. Reduce criminal activities that impact DON operations.

NCIS leverages investigations, collection, operations, analysis, law enforcement, and physical security to inform and advise Navy and Marine Corps commanders concerning threats and vulnerabilities at permanent and transient locations and transit chokepoints.

7.3 MULTIPLE THREAT ALERT CENTER

The NCIS Multiple Threat Alert Center (MTAC) is an analysis and production center for terrorist, criminal, CI, and security information. The MTAC produces threat and trend analyses for afloat and ashore DON commands using data obtained from NCIS special agents worldwide, the U.S. intelligence community, other governmental and law enforcement agencies, and open-source reporting. These products may prove valuable during the mission-planning phase of an operation or exercise. A complete list of available products and services is available via the NCIS SIPRNET home page http://www.ncis.navy.smil.mil, and include:

1. Blue Darts. Time-sensitive messages to warn units and installation commanders of a credible report of an imminent terrorist attack against their unit or installation.

2. Spot Reports. Time-sensitive messages in response to specific FP and terrorism threats that are tailored to alert potentially affected DON assets.

3. Special Analytic Reports. Ad hoc reports that fuse criminal, cyber, CI, and antiterrorism information from various organizations within NCIS. These reports are the main product of the MTAC.

4. Daily Threat Summaries. Daily finished intelligence report assessing current worldwide asymmetric threats that could potentially impact DON interests.

5. Threat Assessments. Tailored assessments for permanent and transient DON assets, that cover terrorist, criminal, foreign intelligence, and medical threats. TAs are typically produced within 30 days of a port visit, in coordination with NCIS field offices.

6. Force Protection Notifications. Initial unclassified notifications on issues of potential interest to commanders, used to assist in force protection decision-making. Force protection notifications are disseminated rapidly to a broad customer base and are posted to Commander, Navy Installations Command's information sharing suite.

7.4 SUPPORT TO ASHORE INSTALLATIONS

NCIS maintains offices at all major Navy and Marine Corps installations. Ashore commanders have direct access to NCIS support and services through 13 field offices and 150 field elements worldwide. NCIS participates in the Joint Staff Integrated Vulnerability Assessment Program, the Chief of Naval Operations Installation Vulnerability Assessment Program, and the Port Integrated Vulnerability Assessment Program via its security training assistance and assessment team (STAAT). STAATs leverage human, analytic, and technological capabilities through advanced collection and analysis in order to enhance our ability to anticipate and identify changes that will influence or potentially threaten DON interests.

7.5 SUPPORT TO AFLOAT COMMANDS

Agents conduct routine visits to expeditionary ports, airfields, and exercise areas through the NCIS Country Referent Program in order to establish and maintain working relationships with U.S. and foreign law enforcement, military, and intelligence counterparts, and to prepare TAs for transiting units. Collection efforts are typically conducted within 30 days for moderate-, significant-, and high-threat countries and within 90 days for low-threat locations. TAs are issued at least 10 days prior to the transiting unit's arrival. In many cases, NCIS special agents are available to directly support transiting units.

7.6 OTHER U.S. INTELLIGENCE COMMUNITY RESOURCES

Although NCIS is the primary source for asymmetric threat intelligence for the DON, OPSEC program managers should always attempt to get threat information through their command's intelligence officer first. However, there are many other agencies and resources available through the U.S. intelligence community. The following agencies are a few potential sources of information that can be used in the OPSEC process to better inform threat analysis in a command's operational environment.

The Office of Naval Intelligence provides maritime intelligence products to the DON and DOD. They specialize in the analysis, production, and dissemination of vital, timely, and accurate scientific, technical, geopolitical, and military intelligence information. The primary source for Office of Naval Intelligence products for operational forces is the Nimitz Operational Intelligence Center.

The DIA is a DOD combat support agency. The DIA is a major producer and manager of foreign military intelligence. They provide military intelligence to warfighters, defense policymakers, and force planners in the DOD and the intelligence community in support of U.S. military planning and operations and weapon systems acquisition.

The FBI provides investigative services for the Federal Government, and focuses on domestic and international terrorism, cybercrime and terrorism, weapons of mass destruction, CI, organized crime, and violent crime. The FBI is provides information on the major and prevailing threats to U.S. citizens and interests.

The Central Intelligence Agency keeps the nation safe by preempting threats, and by furthering U.S. national security objectives by collecting intelligence and producing objective all-source analysis. Central Intelligence Agency products, such as the World Intelligence Review, may provide information helpful to threat analysis.

The U.S. Department of State provides region-specific intelligence on international crime and terrorism threats to U.S. personnel and interests. They provide valuable resources, such as Country Reports on Terrorism and official travel warnings, to units and commands that deploy to foreign soil.

INTENTIONALLY BLANK

CHAPTER 8

The OPSEC Program Manager and Public Affairs Officer Relationship

8.1 OVERVIEW

Effective planning and execution of public affairs (PA) activities are critical to accomplishing a commander's mission. The success of both depends on sound leadership and guidance. Successful PA is important in order to fulfill the public's right to know and to maintain trust and confidence. Credible PA activities are necessary to support the commander's mission and keep the public informed throughout the range of military operations.

8.2 OPSEC AND PUBLIC AFFAIRS: DIFFERENT ROLES

PA's principal focus is to provide information to the American public and international audiences, in support of combatant commander public information needs at all operational levels. The purpose of OPSEC is to reduce the vulnerability of U.S. and multinational forces from successful adversary exploitation of critical information. Figure 8-1 depicts the differences between the roles of PA and IO.

While it appears that OPSEC's and PA's objectives are at odds with each other, both are more successful when they work together. There is a great deal of middle ground between publicly releasing everything and publicly releasing nothing. Neither end of the spectrum is desirable, and much can be released without giving our adversaries an advantage.

Every command should have a formal review process before releasing any information to the public. This review process should include the OPSEC program manager and any other relevant activities to ensure that critical information or indicators are not inadvertently released to the public.

The PAO holds a unique position in the command, with visibility on publicly released information across the entire command. Consequentially, the PAO is often the first person to identify aggregation risk when reviewing information for public release. However, the OPSEC program manager must work with the subject matter expert to determine how to mitigate aggregation risk.

The OPSEC program manager should ensure that the PAO and the rest of the public affairs team are aware of what is on the command's critical information list. The PAO and OPSEC program manager should discuss at what level of detail items on the CIL can be discussed and then document the agreed-upon language. When the PAO and the OPSEC program manager cannot agree upon the level of detail to release on a topic, they should carefully consider and discuss if the risk of releasing the information is greater than the public's need to know, and then determine how to best mitigate the risk. If they cannot come to an agreement, they should bring their concerns to the command's executive officer (XO) and commanding officer (CO). A formal review before release of information would better protect operations while ensuring the widest dissemination of publicly consumable information.

	Target Audience	Intent	Method
PAO	Public	Inform	Public Release
IO (OPSEC)	Adversary	Deny	Five-Step Process

Figure 8-1. Public Affairs and Information Operations Roles Table

8.3 CONCLUSION

To the maximum extent possible, the PAO and OPSEC program manager should coordinate the public release of information relative to the mission or to impending potentially sensitive activity. In close coordination with the PAO, OPSEC program managers must be active participants in the process of deciding what information should be released to the public, balancing the legitimate information requirements of DOD and civilian audiences against the intelligence desires of the enemy. The critical information list should be provided to the PAO. The commander has the ultimate responsibility for assessing whether or not information is releasable from the perspective of both traditional security and OPSEC. For more information regarding public affairs policy, see SECNAVINST 5720.44C Change 1.

CHAPTER 9

OPSEC Guidance for the Navy Ombudsman and Marine Corps Family Readiness Officer

9.1 SCOPE

This chapter discusses OPSEC considerations for the Navy ombudsman and Marine Corps family readiness officer (FRO). It provides an overview of sensitive yet unclassified information on the Internet and how, through data aggregation, it can lead to disclosure of EEFI and—potentially—critical information. Portions of this chapter, in conjunction with appendix M, provide guidance for ombudsman and FRO OPSEC awareness training during predeployment gatherings, family or spouse support meetings, and ombudsman and FRO-sponsored Web pages.

9.2 OMBUDSMAN AND FAMILY READINESS OFFICER PROGRAMS

The Navy Family Ombudsman and FRO programs provide an important communications link between Service member families and Navy or Marine Corps commands. The commanding officer personally selects the ombudsman or FRO, who is an official representative thereof, and serves as the liaison between command families and the command. Most command leaders agree that an effective ombudsman or FRO is a priceless asset, linking commands and families to ensure accurate and timely communication.

Navy and Marine Corps Family Service Centers provide formal ombudsman or FRO training regarding support mechanisms available to assist command family members. Although not a counselor or a social worker, through training or personal experience the ombudsman or FRO frequently assists Service members who have problems.

Commanding officers correspond with their ombudsman or FRO to exchange information. Their communiqués are sources of morale boosters while deployed or separated. Similarly, this communication can dispel rumors or clarify information heard “through the grapevine.” It is critically important that the ombudsman or FRO understands and practices OPSEC and serves as an advocate on the topic to family members. The compromise of one or more elements of sensitive, unclassified information or data could damage a ship’s or activity’s security through the process of aggregation. Just because information is not classified does not mean that it would not be useful to our adversaries. Seemingly insignificant pieces of information put together can often reveal capabilities or intentions that could possibly endanger a mission or lives. Online, it could be what one says over the course of weeks or months being pieced together.

9.3 SOCIAL MEDIA

Despite stringent OPSEC requirements, sensitive information regarding deployed units is readily available on the Internet. Ombudsman and FRO or family support group newsletters published on the Internet or sent via e-mail, as well as unofficial Navy and Marine Corps-related Web sites, augment this information. Hundreds of social media sites and applications also allow family and Service members to stay connected, regardless of their location in the world. These Internet resources make it possible for an adversary to compile sensitive information concerning unit morale, location, organization, personnel, and family members. Even a minor attack against Navy and Marine Corps family members in CONUS would have immediate and significant psychological effects on military forces and combat readiness both in CONUS and overseas.

The use of social media sites such as Facebook or Twitter for online family groups is permitted and encouraged as long as they follow OPSEC best practices. Official sites require an OPSEC review process prior to posting; but family-related sites do not, however, but are strongly encouraged to go through some form of OPSEC review process. Despite these safeguards, hyperlinks and comments other people post often facilitate the collection of additional information that, when combined, reveal critical information. An example of this follows:

> An article published in the Wall Street Journal on military blogs provided links to official and unofficial military Web sites. Using Web links featured in this article, the CI Field Activity (West) accessed a blog entitled Journal of a Military Wife. The blog provided information concerning the author's spouse, his unit, and hyperlinks to family support group newsletters. Although an alias was used in the blog, the true name of the author, contact phone number, and e-mail address were easily obtained by accessing the command's family support group newsletter through a hyperlink provided in the blog. Basic information was obtained from the Internet and combined with details about the unit available from two unofficial military Web sites, Global Security and Military.com, a comprehensive snapshot of the unit was developed to include its assigned personnel and their families.

9.4 INFORMATION OBTAINED

Unclassified open-source data can be obtained from social media, family support group newsletter sites, unofficial military Web sites, and online white pages revealed information corresponding to the unit's EEFI:

1. Unit-related Information.

    a. Organization of the unit, to include key leadership, names, and ranks of assigned personnel and unit home stations.

    b. Partial unit rosters for the headquarters unit and subordinate elements that included name, rank, and position of assigned personnel.

    c. Unit travel information (e.g., unit deployed from California to Camp Virginia, Kuwait, and later moved to Navistar, outside Basra, Iraq).

    d. Photographs of soldiers assigned to the unit, complete with names and rank identification.

    e. Daily training schedule for the supply and maintenance section.

    f. Manning and position roster for the maintenance and supply section.

    g. Mission of the headquarters and subordinate units.

    h. Force protection mission of a unit.

2. Military Member-related Information.

    a. Photographs of soldiers with family members identified by name.

    b. Route of travel for unit soldier on leave (e.g., Iraq to Dublin, Ireland; to Dallas, TX; to Sacramento, CA).

    c. Contact information for family members of deployed soldiers to include phone numbers, e-mail addresses, and residential addresses.

    d. Biographical information on soldiers to include rank, military specialty, age, marital status, family members, and home of record.

    e. Personal information regarding a military member's relationship difficulties with spouse and parents.

9.5 MULTIPLE USES OF INFORMATION

Terrorist groups have used information gained from the Internet to target family members of deployed military personnel. In countries throughout the Middle East and southern Asia, terrorists have successfully kidnapped and assassinated numerous westerners in an attempt to influence U.S. foreign policy. To escalate this threat, terrorist organizations such as Al-Qaeda, The Islamic State of Iraq and the Levant, and Boko Haram have threatened to employ similar tactics in the United States. A successful attack against a military family member in the United States would have extensive psychological impact. An attack, or even the threat of an attack, would undermine public confidence in the U.S. Government's ability to protect them at home, decrease combat effectiveness of deployed military personnel concerned with safety of their family members, and negatively affect deploying Service members.

Criminal groups have used personnel information found on social media and on military Internet sites to target deployed personnel's family members for fraud, burglary, or other criminal activity. For example, a recent legitimate program to provide free computers to family members of deployed Service members required a copy of the Service member's deployment orders, home address, and phone number. Most family members readily provided the information. A criminal could use the same tactic to obtain information from family members to conduct identity theft or other nefarious activities. This is another reason commanders must assure their OPSEC training and awareness program include educating families.

Military and personal information gathered from the Internet provides Foreign Intelligence Service a "least intrusive means" of determining placement and access during the spotting and assessing of potential sources. Personal information gathered from the Internet could also serve as the foundation for possible Foreign Intelligence Service exploitation operations.

9.6 SOCIAL MEDIA COUNTERMEASURES

Criminals and terrorists use personal information posted on public Web sites to target individuals. In most cases, applying countermeasures to safeguard against exploitation of sensitive information is very simple. It is possible to highlight our Navy and Marine Corps personnel for the great work they do; however, refrain from being too specific. With very little information, adversaries can quickly locate addresses or other personal information about our employees. The following are some generic countermeasures that will help prevent adversaries from gaining too much insight to personnel and activities.

1. Limit personal information. Identifying an individual by name, rank, and organization along with a picture can be very useful to adversaries. Limit the information by removing the individual's name, or refrain from including a picture with the information.

2. Speak in generic terms. If publishing information about a project or activity, do not go into details.

3. Avoid vanity Web sites or pages. Refrain from putting out information that touts people, projects, activities, etc.

4. Post only information you own. Refrain from duplicating information already contained on another DOD Web site. Hinder data aggregation, and avoid long-term archives on public sites. Do not make your site a one-stop shop for the adversary.

5. Avoid overloading your Web site with numerous tabs and pages. Keep your Web site to a manageable and user-friendly size.

Remember: It is not just patriotic Americans viewing our public Web sites. There are many individuals and organizations collecting information about us who intend to use it to their advantage and our detriment. We must not make their job easy.

INTENTIONALLY BLANK

CHAPTER 10

Social Media

10.1 OVERVIEW

As social media becomes more prevalent and integral to mass communication and public affairs, the military will use social media and Web-based presences to communicate with Service members, families, and the public at large. Social media provides the DON with a more convenient and timely avenue for communication. Social media and Web-based presences allow worldwide access to unprecedented amounts of information that can be both helpful and harmful to DON commands, missions, and activities. In order to facilitate the growing demand for information and participation in social media, commands are encouraged to establish social media presences. Along with providing families and Service members with up-to-date and timely information, social media also allows the public to interface with its naval forces. This, however, opens the door to more nefarious entities that wish the DON and its families harm. Units must exercise caution and apply the OPSEC process to the use of social media and Web-based presences in order to achieve maximum information output and maintain a strong and secure operational posture.

10.2 ACCEPTABLE SOCIAL MEDIA USE

There are thousands of social media sites on the Internet, and more are being created every day. Although there is no list of DON-approved social media sites, the General Services Administration has negotiated "Federal-friendly" terms of service agreements with several social media sites. These General Services Administration-negotiated sites have terms of service agreements that enable appropriate use. It is recommended that units use Federal-friendly social media sites. A list of these sites can be found at https://www.digitalgov.gov/resources/negotiated-terms-of-service-agreements/. Commonly used social media sites can be found on the Services' home pages. For more information on social media use, contact the Chief of Naval Information.

Commands are encouraged to establish a controlled and monitored social media presence to support their activities, personnel, and families. When establishing a social media presence, commands should appoint a manager of their social media sites. This manager should control the release of information and posts on the command's social media sites. Before any information is posted to a social media site, the appropriate authority for release should vet and approve it. The vetting process for the release of information should include personnel review, through which useful recommendations as to whether or not information should be released can be made. People who can make such recommendations may include the OPSEC program manager, personnel from operations, public affairs, intelligence, security, or any other OPSEC-trained personnel. Commands should establish well-defined vetting processes that fit their mission and protect their critical information from public release. Commands mitigate risk to their mission and personnel by incorporating a vetting process into all information released via social media. A flow chart that helps to determine what to post can be found in appendix O.

For many commands, social media is primarily used to interface with family members and to provide them with the most up-to-date information about their Service member. This is encouraged. Commands should post often and post accurately; this encourages families to go to the official command social media page for their information and prevents them from searching elsewhere or creating other pages for information sharing. If nonofficial pages are created for information sharing, then the command has no control over what information is posted to that social media site. This could increase the risk to the command's mission by unintentionally releasing critical information. Commands should also monitor what others post to the command's social media sites; commands are able to remove any posts of critical information, indicators, or questions that may lead to posting of sensitive information by doing this. History has shown that well-managed, well-maintained social media sites have prevented the release of critical information while on deployment.

10.3 THE DANGERS OF SOCIAL MEDIA

In spite of all the good that comes from using social media, its method of delivery inherently makes its use a risky venture. The avenues that social media creates for communication become new attack vectors for potential adversaries. As you are reading this publication, adversaries are attempting to collect information on the DON and its commands and activities. The easiest way for an adversary to collect critical information is via the Internet. Commands create a potential source for adversaries to collect useful and actionable information by creating a social media page. However, this does not mean that commands should not have a social media presence. As long as commands can identify critical information, threats, vulnerabilities, and countermeasures, commanders can make calculated decisions as to how much risk to assume when using social media.

Adversaries will look to see who is associated with a command’s social media page. Adversaries seek this information for multiple reasons; they may want to use an associated individual’s social media page to gain information, extort information from individuals associated with the command using phishing and social engineering, or worse, they may be looking to harm individuals associated with the command. A command can mitigate these dangers by making a group private and allowing access to the group by invitation only.

Cyber criminals are also a threat to military members and their families. Cyber criminals seek to gain information about an individual in order to attain some sort of monetary gain from the individual. This could come in the form of stealing personally identifiable information (PII) such as banking information, social security numbers, passwords, usernames, birthdates, or family information. Because social media inherently is an information sharing platform, cyber criminals will use it to obtain or steal an individual’s critical information. A command can help prevent cybercrime against their Service members by refraining from posting any PII or information about specific Service members or their families onto their social media pages. Commands should also ensure that their Service members and their families are aware of the dangers of cyber criminals and social media. This will help to ensure that they are deployable and prepared for any mission.

10.4 INFORMATION AGGREGATION

Cyber criminals or adversaries of the U.S. Government rarely obtain all their information from one source. A command’s social media page on its own will most likely not provide an adversary the information they need to disrupt a command’s mission. However, when adversaries are able to aggregate information from multiple sources they may be able to gain a clear understanding of a command’s mission and information critical to the accomplishment of that mission. This danger does not mean that a command should not use social media to communicate with Service members, families, and the public. As long as commands are responsible and apply the five-step OPSEC process to their employment of social media, they can mitigate threats to an acceptable level of risk. The proper use of social media as an information sharing tool can increase a command’s family readiness and mission effectiveness. For more information on the use of social media, refer to the DON Social Media Handbook and the Marine Corps Social Media Handbook.

Social media should be used to update families and the public on the actions of a command. The DON and its actions are legitimate and inherently good for the American people. We strengthen the position and resolve of our naval forces by openly, honestly, and carefully sharing our actions with the American people.

CHAPTER 11

OPSEC Planning

11.1 THE OPSEC PROGRAM AND OPSEC PLANNING

Much of this publication discusses how to develop an OPSEC program at a command or unit. However, there is more to OPSEC than just building a program. OPSEC must be included with operations planning at the strategic, operational, and tactical levels of war. Naval personnel conduct most of the planning at the tactical and operational levels. A command's OPSEC program and critical information list are usually not sufficient to satisfy planning for specific operations or plans, though. A command's OPSEC program sets a baseline for protecting critical information. However, the critical information list that is part of a command instruction includes only general information rather than information that is specific to an operation or plan. In order to properly apply the OPSEC process to planning efforts and specific operations, OPSEC must be included in the planning process.

One of the main objectives of IO is to achieve information superiority over the adversary. Information superiority is the operational advantage derived from the ability to collect, process, and disseminate an uninterrupted flow of information while exploiting or denying an adversary's ability to do the same. Within IO, one of the main objectives of OPSEC is to achieve essential secrecy, a vital aspect of achieving information superiority. Essential secrecy is a condition achieved by the effective denial of distinguishable aspects of friendly operations. OPSEC planners work to achieve essential secrecy within a plan, which enables the commander to achieve information superiority.

11.2 OPSEC IN THE PLANNING PROCESS

The planning processes of the Navy and Marine Corps are very similar, and OPSEC is included similarly in both. OPSEC planners have to integrate OPSEC into each step of the planning process and coordinate closely with other planners, specifically those who coordinate and task the other IRCs. In order to facilitate the IRC integration process, the OPSEC planner should sit in the IO cell. Much of the work of an OPSEC planner must be completed and delivered as products to be considered during the course of action (COA) development, COA war game and analysis, and COA comparison and decision. Consequently, the majority of an OPSEC planners work must be completed during the problem framing or mission analysis steps of the planning process. The planning estimates that the OPSEC planner develops are vital inputs to COA development and COA decision steps of the planning process. In war, a commander must know what the adversary can understand about friendly operations and activities in order to make a fully informed decision. The commander must be able to consider the OPSEC implications of each COA before a decision can be made on which COA to approve for an operation.

The critical information identification and threat analysis steps of the OPSEC process should be conducted during the mission analysis or problem framing steps of the planning process. In the mission analysis or problem framing phase of the planning process, OPSEC planners must work from guidance from higher commands in order to conduct OPSEC mission analysis, critical information identification, and threat analysis. During the OPSEC mission analysis, an OPSEC planner must take all higher guidance and orders and develop a staff estimate to provide to the IO cell, planning working group, and commander, if necessary. In order to identify the critical information and indictors associated with a plan, the OPSEC planner may need to identify OPSEC tasks; develop an OPSEC mission statement, operational profile, and critical information and indicators list; and analyze friendly activities. In order to analyze threats to a plan's information, the OPSEC planner may need to work with their intelligence section to analyze all potential adversaries, conduct a conduit analysis, and develop a profile of the information environment. Completing the first two steps in the OPSEC process allows an OPSEC planner to develop a written staff estimate that clearly outlines the role that OPSEC plays in COA development and the plan as a whole.

The vulnerability analysis and risk assessment steps of the OPSEC process should be conducted during the COA development and COA war game and analysis phases of the planning process. As operations planners develop COAs, OPSEC planners must conduct a vulnerability analysis and risk analysis for each potential COA. OPSEC planners may need to conduct a friendly activity analysis to determine which activities are vulnerabilities. These vulnerabilities should then be compared to adversary's intelligence collection capabilities and critical information list to determine the level of risk for each COA.

During the COA war game or comparison phase of the planning process, OPSEC planners identify and apply countermeasure for each COA. This involves developing a concept of operations for OPSEC and subsequent OPSEC activities, tasks, and timelines. In this portion of the process, the OPSEC planner develops the actions that the unit will take in order to achieve essential secrecy.

The many planning products that OPSEC planner develops should then be compiled and summarized as a part of the COA briefs to the commander. OPSEC considerations should be a part of the commander's decision-making process for the plan, operation, or mission. Once a COA is decided, the OPSEC planner must then translate their work into a section of the operations order. The OPSEC part of the plan or order should be included as Tab C (Operations Security), to Appendix 3 (Information Operations), of Annex C (Operations). A sample Tab C (Operations Security) is provided in appendix D of this publication.

11.3 FOCUS ON ADVERSARY INTELLIGENCE COLLECTION

Much of the OPSEC planning in an OPSEC program is focused on a large set of adversaries. This is because an OPSEC program establishes an OPSEC baseline to protect against a large number of potential threats. However, a plan, operation, or mission allows the OPSEC planner to be more focused in the threat analysis. Just as they do during the normal OPSEC process, an OPSEC planner must work closely with their intelligence section to have a full understanding of the adversary's capabilities and intent. Specifically, the planner must understand specific collection capabilities and systems, and what vulnerabilities those systems and capabilities could exploit. Countermeasures must then be applied to specific collection capabilities and systems in order to protect specific vulnerabilities. This is a much more detailed process than what a standard OPSEC program requires.

When analyzing adversary intelligence collection, consideration must be paid to the adversary decision maker. It is not enough for the adversary to collect information; they must then process, analyze, and disseminate intelligence products. Additionally, the collected information and subsequent intelligence products often must traverse bureaucratic lines of communication before they reach the adversary decision maker who can act on the intelligence. These processes take time and should be considered when analyzing the adversary's ability to operate in the information environment. The ultimate goal of OPSEC is prevent the adversary decision maker from understanding vital aspects of the plan, operation, or mission.

11.4 DISTINGUISHABLE ASPECTS OF FRIENDLY OPERATIONS

Adversaries are continually attempting to collect information on friendly activities and units. During a planned operation or mission, adversaries attempt to collect information to understand specific aspects of friendly operations. If an adversary is able to understand specific aspects of our operations, they can disrupt our plan. The distinguishable aspects of friendly operations that should be considered are: presence, capability, strength, intent, readiness, timing, location, and method. These are the aspects of the plan, operation, or mission that the OPSEC planner should attempt to conceal.

Presence is the current physical or virtual placement of a unit within an operational environment. An adversary might desire to know which units exist in specific environment and which units do not. This information can become particularly useful when coupled with information about the unit's strength, capability, or intent. When viewed in contrast, the presence of a unit in an environment can also indicate intent, method, or timing. Although a unit's presence may be difficult to conceal, OPSEC planners must consider how an adversary can use presence when viewed within the context of the rest of the information environment.

Capability is the resources or functions that enable the execution of a particular kind of military action. This aspect of operations is closely related to strength, but differs in that it describes what type of actions a particular unit can execute. An OPSEC planner should note that different units have different functions and capabilities. The mere presence of a specific unit in the operational environment may also reveal specific capabilities of the military force.

Strength is the aspect of friendly activities that describes the capacity to carry out a capability. Though this aspect is similar to readiness, it deals more with force levels. One can consider it as a percentage of strength compared to the level necessary to carry out a specific task or function. To the OPSEC planner, strength is important to consider because an adversary can determine how much of a function they can bring to bear in the operational environment.

Intent is what a military force must do and the conditions the military force must establish in order to accomplish the mission. This is closely related to the commander’s end state. The adversary can understand the very nature and purpose of a military force’s mission by understanding the intent.

Readiness is the ability of a military force to fight and meet the demands of an assigned mission. This can also be considered how quickly a military force can bring its assets to bear in the operational environment. If an adversary can determine a unit’s readiness, they may be able to determine how quickly they can respond to adversary actions.

Timing is the “when,” or chronological sequence of actions. Disclosure of timing can be especially damaging to a mission or plan because it can reveal to the adversary when specific actions are to take place in the operational environment. This allows an adversary to plan their activities around the planned operation or mission. An OPSEC planner must carefully assess how to protect timing and the cost it can have to a bigger plan.

Location is the projected physical or virtual positon where a force acts to achieve a desired effect. Although this aspect is simple in nature, it is of extreme value to the adversary.

Method is how forces accomplish the intended objective; the operational approach to the mission. If an adversary correctly pieces together the friendly method for achieving an objective, they may develop a plan to seize the initiative at multiple points along the friendly line of effort. OPSEC planners usually focus heavily on protecting the method of a plan, operation, or mission.

These aspects of the operation may have different values associated with them that dictate the amount of resources a planner should dedicate to protecting them. Additionally, planners may not be able to protect some aspects of an operation. Still in other cases, planners may want the adversary to see certain aspects of an operation. It is important to work with deception planners to understand which aspects of a plan, mission, or operation should be protected.

It is vital for an OPSEC planner to conduct a thorough analysis of the distinguishable aspects of friendly operations. It is from these distinguishable aspects that the planner develops their critical information and indicators list. Information and indicators that reveal distinguishable aspects of friendly operations become critical to mission success. A planner should also understand how the adversary can understand aspects of friendly operations. An aspect such as timing may be useless when viewed in isolation, but can have significant meaning when viewed in the context of other aspects such as location or method. OPSEC planners must view OPSEC in the context of the information environment and not as an isolated aspect of planning in order to have this thorough understanding of distinguishable aspects of an operation.

11.5 FROM ESSENTIAL SECRETS TO INDICATORS

Much of the OPSEC planning in an OPSEC program is focused on a large set of adversaries. This is because an OPSEC program establishes an OPSEC baseline to protect against a large number of potential threats. However, a plan, operation, or mission allows the OPSEC planner to be more focused in the threat analysis. Just as in the normal OPSEC process, an OPSEC planner must work closely with their intelligence section to have a full understanding of the adversary’s capabilities and intent. Specifically, the planner must understand specific collection capabilities and systems and what vulnerabilities those systems and capabilities could exploit. Planners must then apply countermeasures to specific collection capabilities and systems in order to protect specific vulnerabilities. This is a much more detailed process than what a standard OPSEC program requires.

The OPSEC planner must determine what the essential secrets are for the plan, operation, or mission. This involves analyzing which distinguishable aspects are critical to the mission's accomplishment. The essential secret is the critical distinguishable aspects of a specific operation. The essential secret can also be used to develop the OPSEC mission statement for the plan, operation, or mission.

> Example of an essential secret: The capability, intent, timing, and location of amphibious operations near the coast.
>
> Example of an OPSEC mission statement: On order, the Marine Expeditionary Unit will protect the capability, intent, timing, and location of amphibious operations near the coast.

Once an essential secret is determined, the OPSEC planner must conduct a friendly activity analysis in order to determine which activities may reveal the essential secret to the adversary. Each friendly activity has signatures associated with it. Signatures are events or actions that must happen in order to execute a friendly activity. These signatures may deviate from the unit's baseline operations and project information or indicators into the information environment. The information and indicators of friendly actions that an adversary can observe and use to disrupt friendly actions are critical information and indicators. If an adversary cannot observe the information or indicators, then they are not critical and likely do not require the protection of a measure or countermeasure. The critical information and indicators derived from the friendly activities of an operation are used to inform the critical information list for the plan, mission, or operation.

11.6 OPSEC TASKS

An OPSEC planner must determine how to prevent the adversary from collecting that information after critical information and indicators associated with friendly activities are identified. This will often require the application of OPSEC measures or countermeasures. Countermeasures tend to focus on adversary collection capabilities, whereas measures focus on friendly activities. In planning, OPSEC measure and countermeasures are identified as tasks such as protect, disrupt, deny, or destroy. An OPSEC measure or countermeasure is created by combining a task with a target and a time period. The OPSEC measure or countermeasure can then be translated into a task. Adding an executing unit to a measure or countermeasure creates an OPSEC task.

> Example of an OPSEC task: From landing day–21 to landing day, the maritime raid force conceals the hydrographic survey and reconnaissance supporting phase II amphibious operations.

OPSEC tasks are the execution part of an OPSEC plan. However, the OPSEC planner does not have operational control over any assets or units. The OPSEC planner needs to work with other members of the planning team to develop realistic and executable OPSEC tasks. This requires significant coordination with other planners to ensure that OPSEC tasks are considered and executed.

APPENDIX A

OPSEC Checklists

A.1 U.S. NAVY AFLOAT STAFF

1. Is a strike group staff OPSEC program manager assigned?

    a. Is the strike group staff OPSEC program manager appointed in writing?

    b. Has the strike group staff OPSEC program manager attended the Navy OPSEC course or IOSS program manager's course?

    c. Has the strike group staff OPSEC program manager completed OPSE 1301?

    d. Has the strike group staff OPSEC program manager coordinated with other command security managers (COMSEC, INFOSEC, computer security (COMPUSEC), SSO, etc.)?

    e. Has the strike group staff OPSEC program manager coordinated with other significant staff personnel (PAO, master-at-arms (MAA), AT/FP, senior officer present afloat (SOPA), legal, etc.)?

2. Are OPSEC program managers assigned or designated onboard strike group units?

    a. Are the ship's OPSEC program managers appointed in writing?

    b. Has the ship's OPSEC program manager attended the Navy OPSEC course or IOSS program manager's course?

    c. Has the ship's OPSEC program manager completed OPSE 1301?

    d. Has the ship's OPSEC program manager coordinated with other command security managers (COMSEC, INFOSEC, COMPUSEC, SSO, etc.)?

    e. Has the ship's OPSEC program manager coordinated with other significant command personnel (PAO, MAA, AT/FP, SOPA, legal, etc.)?

3. Meet with all strike group OPSEC program managers a minimum of 180 days prior to deployment (or as feasible) to discuss operations and missions, and task each with developing their unit's critical information.

4. Meet with all strike group OPSEC program managers a minimum of 90 days prior to deployment in order to identify the strike group's and each individual unit's critical information.

5. Has a Web Risk Self-Assessment been conducted for each unit in the strike group?

6. Task each unit with conducting an OPSEC assessment a minimum of 60 days prior to deployment and ensure that they report their completion date to strike group or staff OPSEC program manager.

7. Ensure that each unit conducts a predeployment briefing for ombudsmen or family members a minimum of 30 days prior to deployment and that they report completion to the strike group or staff OPSEC program manager.

8. Depending of assignment of units, ensure that each unit conducts an annual assessment and that they report their completion date to their ISIC.

A.2 U.S. NAVY INDIVIDUAL UNIT OR SHORE COMMAND

1. Is a command OPSEC program manager assigned in writing?

    a. Is the appointee from the command Plans or Operations department?

    b. Does the appointee have a projected rotation date greater than one year, or a relief identified under training?

    c. Are the OPSEC program manager and department representatives aware of their responsibilities?

    d. Does the OPSEC program manager attend command security awareness and education meetings, and address OPSEC issues?

    e. Has the command OPSEC program manager attended or requested to attend the Navy OPSEC course or IOSS program manager’s course?

2. Has the OPSEC program manager established a continuity binder?

    a. Are current editions of all instructions, pamphlets, and directives (DOD 5205.2, JP 3-13.3, OPNAVINST 3432.1 series) being maintained in support of the OPSEC program?

    b. Does the command have local directives that define command OPSEC program requirements, responsibilities, and procedures?

3. Does the commander actively advocate, support, and implement OPSEC options in support of the operational mission and exercises?

    a. Has the commanding officer signed an OPSEC policy letter supporting the program?

    b. Is the command’s critical information reviewed and approved by the commanding officer?

    c. Is the command’s critical information list available to all command members?

4. Does the command OPSEC program promote the active participation and involvement of all personnel?

    a. Are OPSEC posters prominently displayed throughout the command?

    b. Are all avenues of media being utilized to promote OPSEC (internal local area network (LAN), site television (TV), plan of the day (POD), etc.) ?

    c. Are OPSEC education materials reaching all command members?

    d. Is the command critical information list tailored to each functional activity?

        (1) Is the critical information list specific, realistic, and current?

        (2) Are command or functional area critical information lists easily accessible to command members?

(3) Are command members familiar with command or functional area critical information?

(4) Is the critical information list unclassified to allow for maximum dissemination?

5. Does the command OPSEC program include provisions for reviewing plans, OPORDs, and exercise scenarios?

a. Is the current (less than 12 months) potential adversary threat data maintained and considered in plans and exercises?

b. Do command instructions, plans, doctrine, or OPORDS contain, at a minimum, the purpose and current definition of OPSEC, OPSEC threat, and critical information?

6. Are the interrelationships of OPSEC, COMSEC, cybersecurity, physical security, and information security programs clearly understood by the OPSEC program manager?

7. Has the command OPSEC program manager coordinated with other command security managers (e.g., COMSEC, INFOSEC, cybersecurity), as well as command supply and PA, to incorporate OPSEC concepts and lessons learned into security training sessions?

8. Has the command OPSEC program manager continually liaised with the staff or higher headquarters OPSEC program manager?

9. Is OPSEC training related to the command mission, tailored to individual duties and responsibilities, and presented to newly assigned personnel within 30 days after their arrival for duty?

10. Does command OPSEC training contain the following?

a. The OPSEC methodology

b. Duty-related mission critical information and OPSEC indicators

c. Threats to the unit mission

d. Individual responsibilities

e. OPSEC and its relationship to other information-related capabilities.

11. Does the OPSEC program manager review command OPSEC instruction annually and, if required, submit an annual OPSEC Status Report to their respective staff?

12. Has an internal OPSEC assessment been conducted within the last year?

a. If YES, then:

(1) When?

(2) Are the results easily accessible?

(3) Have results been addressed through awareness programs?

(4) Has unit mission or critical information changed significantly to warrant a new assessment?

b. If NO, then:

(1) Has one been scheduled or requested?

13. Have actions been taken to act on recommendations or to correct weaknesses and deficiencies noted in the OPSEC assessment?

14. Are all OPSEC recurring publications (e.g., the OPSEC update, COMSEC quarterly analyses, etc.) reviewed for OPSEC lessons learned?

15. Do official and unofficial feedback publications (such as command newsletters and Web sites) contain sensitive or critical information? If so, are they protected? Who reviews them for OPSEC compliance?

16. Has a Web Risk Self-Assessment been conducted on the command’s Web site? If yes, when?

17. Do indexes for directives and operating instructions reveal sensitive operations or functions?

18. Do unclassified computer products disclose sensitive mission activity?

19. Is the OPSEC program manager on distribution for telecommunications monitoring reports (joint communications security monitor activity) involving their command?

20. Does the OPSEC program manager meet with the command ombudsman to provide training to families? Has family training been incorporated into predeployment briefs?

A.3 U.S. MARINE CORPS INSPECTOR GENERAL CHECKLIST

3070 OPERATIONS SECURITY	
This checklist applies to all Marine units, activities, and commands that prepare, sustain, or employ Marine forces throughout the spectrum of warfare. The application is not limited to operational units.	
Functional Area Sponsor: PP&O, PL, PLI	**Name of Command**
Subject Matter Expert: James J. Sydnor	**Date**
DSN 222-4293 COML (703) 693-4293	**Inspector**
Revised: 23 February 2016	**Final Assessment** **Discrepancies:** **Findings:**
Subsection 1–GENERAL	
0101	Provide a copy of each of the OPSEC Manager’s and/or Coordinator’s signed appointment letter/s. Reference: MCO 3070.2A, par 4a(2)(a) (Authorized signees are the CO, XO, CoS or civilian equivalent)
Results	Comments
0102	For all program managers and coordinators, provide completion certificates for OPSEC fundamentals training. Reference: MCO 3070.2A, par 4c(3)(d) (Training should be completed within 30 days of appointment)
Results	Comments

Figure A-1. U.S. Marine Corps Inspector General Checklist (Sheet 1 of 4)

Subsection 1–GENERAL	
0103	For all program managers and coordinators at the Regimental/Group level and higher, to include supporting agencies/activities, provide completion certificates for resident OPSEC training. Reference: MCO 3070.2A, par 4c(3)(e) (Training should be complete within 90 days of appointment)
Results	Comments
0104	For all program managers and coordinators, public affairs officers, family readiness officers, webmasters, and any other personnel authorized to review information for public release via the internet; provide completion certificates for “web” OPSEC training. Reference: MCO 3070.2A, par 4c(3)(f)1 and DoDD 5205.02E encl 2,11.l (Training should be completed within 90 days of appointment and is not waivable.)
Results	Comments
0105	Provide your current threat analysis that shows the collection methods an adversary may use to obtain your unit’s information? Reference: MCO 3070.2A, par 1c and 4c(7)(c) (Provide copies of worksheets used to determine threat associated with operations, exercises, activities, system development, and test and evaluation in garrison and deployed environments. Use the Threat Value Matrix located in App to encl 4 of DoDM 5205.02-M)
Results	Comments
0106	Based on your vulnerability analysis, provide your vulnerabilities. Reference MCO 3070.2A, par 1c (Provide copies of worksheets used to determine vulnerabilities. Use the Vulnerability Values located in App to encl 4 of DoDM 5205.02-M)
Results	Comments
0107	Based on your risk assessment, provide you risk level before applying countermeasures. Reference: MCO 3070.2A, par 1c (Provide copies of worksheets used to determine level of risk. Use the Risk Assessment located in App to encl 4 of DoDM 5205.02-M)
Results	Comments
0108	Provide your unit’s critical information and is it updated as mission changes? Reference: MCO 3070.2A, par 1c, par 4c(7)(c) and DoDD 5205.02 (Use the Critical Information Value Matrix located in App to encl 4 of DoDM 5205.02-M)
Results	Comments

Figure A-1. U.S. Marine Corps Inspector General Checklist (Sheet 2 of 4)

Subsection 1–GENERAL	
0109 Results	Based on your completion of the OPSEC process, what is your commander’s acceptable level of risk? Reference: MCO 3070.2A, par 1c (Provide documentation that the commander has accepted this level of risk) Comments
0110 Results	What measures/countermeasures are in place to eliminate/mitigate the collection methods of your adversary or to reduce risk to the commander’s acceptable levels? Reference: MCO 3070.2A, par 1c and par 4c(7)(c) (Work with your security manager to de-conflict any conflicts of interest) Comments
0111 Results	Provide supporting documentation of quarterly review of command sponsored social media and official websites. Reference: MCO 3070.2A, par 4b(17)(c)8 Comments
0112 Results	Provide supporting documentation of all command personnel completed annual training. Reference: MCO 3070.2A, par 4c(3)(c) Comments
0113 Results	Show that contract requirements properly reflect OPSEC responsibilities and are included in contracts where applicable. Reference: MCO 3070.2A, par 4b(17)(c)6 Comments
0114 Results	Show how OPSEC is being promoted throughout the command. Reference: MCO 3070.2A, par 4c(10) (i.e. posters, email reminders, part of new join in- briefs, or by any other appropriate means) Comment
0115 Results	Provide a list of all subordinate commands’ OPSEC practitioners one level below. Reference: MCO 3070.2A, par 4b(15)(b) Comments
0116 Results	Provide a copy of the command’s annual review of all subordinate OPSEC programs one level below. Reference: MCO 3070.2A, par 4b(15)(d) Comments

Figure A-1. U.S. Marine Corps Inspector General Checklist (Sheet 3 of 4)

Subsection 1–GENERAL	
0117	Provide a copy of the command’s OPSEC order that is signed by the commanding officer and includes the command’s Critical Information List (CIL). Reference: MCO 3070.2A, par 4b(17)(c)1
Results	Comments
0118	As of July 2013, all units and activities at the regimental/group level and higher are required to retain annual inspection check lists for 3 years. This includes annual inspections conducted on subordinate commands. Provide copies of the annual command level and subordinate command’s annual inspections. Reference: MCO 3070.2A, par 4c(7)(b)2 (All records should be managed according to National Archives and Records Administration as per SECNAV M-5210.1).
Results	Comments

Figure A-1. U.S. Marine Corps Inspector General Checklist (Sheet 4 of 4)

INTENTIONALLY BLANK

APPENDIX B

Essential Elements of Friendly Information

B.1 ESSENTIAL ELEMENTS OF FRIENDLY INFORMATION GUIDELINE

The following list is a general guideline to use in developing essential elements of friendly information (EEFI) for a given activity, mission, or phase of campaign.

1. Information that reveals the specific capability of an organization
2. Information that reveals a weakness or a compromise of a specific operation
3. Knowledge about specific measures used to protect a mission or operation
4. Information that reveals a security weakness of a unit or activity
5. Information that reveals the security classification of various projects
6. Information that associates cover names or nicknames with classified projects, activities, or operations
7. Information that reveals special requirements for a specific duty that could indicate deployment location or mission, including the following:
   a. Special immunization requirements
   b. Unique language requirements
   c. Other-than-routine security clearance procedures
   d. Unusual survival or mobilization training
   e. Extraordinary passport, visa, and foreign clearance requirements
   f. Special or civilian clothing requirements.
8. Special mission equipment of systems information
9. Material about special installation projects, dates, and locations
10. Essential personnel privacy information, to include chain of command.

INTENTIONALLY BLANK

APPENDIX C

Critical Information List

C.1 SCOPE

This appendix provides tools specific to creating a critical information list.

C.1.1 Examples

Pages C-2 through C-4 provide an example of an “all hands” memorandum from an afloat commanding officer to the crew apprising them of their OPSEC responsibilities. It explains that OPSEC is everyone’s responsibility, and provides examples of ship’s critical information that, if compromised, could have adverse effects on the ship’s personnel and, thus, the overall mission. Every attempt should be made to ensure critical information lists are unclassified to enable widest dissemination (i.e., facilitate 100 percent awareness). The example may be used by any activity, afloat or ashore, as it provides a comprehensive list of possible critical information.

MEMORANDUM FOR ALL HANDS

Subj: USS XXXX CRITICAL INFORMATION LIST

1. The success of our mission on board USS XXXX depends on our personnel performing their duties to the utmost of their abilities. Our success also hinges on maintaining operations security (OPSEC). Providing our adversaries knowledge of our strengths and weaknesses could jeopardize the success of our mission and even cost the lives of our shipmates.

2. Knowing what critical information can be harmful if released to our adversaries is key to practicing good OPSEC. To this end, the development and frequent update of a critical information list is vital. It is the responsibility of all hands to know what information is deemed critical in order to avoid its inadvertent disclosure to our adversaries. In conjunction with the OPSEC team, I have designated the following ship's information as critical information:

Specific:

OPERATIONS

a. CIWS MT12 is CASREPD–ETR is six weeks.

b. Command is in FPCON ALPHA.

c. USS XXXX failed INSERV; 6 of 12 MMR boilers are down, flight deck is not certified, and 2 CATS are inoperative until further notice.

d. Ship will arrive in Cairo, Egypt at time/date.

PLANS

a. Unit will break away from the Strike Group on XX date and transit the Turkish straits on date to participate in joint BSO with Ukrainian, Romanian, and Bulgarian forces.

b. Mission with Greek Special Forces in support of the Olympics.

c. NEO mission with U.S. Embassy in Liberia at LOCATION on XX date.

COMMS

a. INMARSAT is down; using HF communications ISO the mission.

b. Password to access the JOTS system.

c. Link 11 and Link 4 communications with surface and air assets are down as a result of a/c problems.

d. Lost the forward WSC–3; SATCOM is limited.

e. TACAN inoperative, flight operations suspended.

INTELLIGENCE

a. The ship's sole language linguist was medically evacuated; we have no VHF voice intercept capability.

b. The map and location of area BRAVO provided by SEAL Team is excellent.

LOGISTICS

a. Parts for both evaporators will take two weeks to arrive. Ship will be on water hours.

b. Ordered 2,000 sets of desert cammies and boots. Scheduled to arrive on date and issued by date.

BUDGET

a. The budget for the mission has been reduced by 40 percent.

PERSONNEL

a. Admiral Jones will depart the USS ship at time/date via CH–53 and should touch down at location at time/date.

b. Only one quarter of the crew received their anthrax vaccines. There are no more doses available throughout DOD.

c. The ship is 20 percent undermanned; 40 percent undermanned in the wardroom and CPO mess.

Generic:

OPERATIONS

a. Status/limitations of personnel, equipment, and weapons systems and key contingency concepts/processes.

b. Operational command and control structure.

c. Any standard operating procedure.

d. Identification, strength, and combat readiness posture of assigned forces.

e. Specific aspects and changes of FPCONS/INFOCONS.

f. Critical ship/activity or regional infrastructure nodes/links.

g. Alert status, response times, and schedules.

h. Exercise/inspection postures and results.

i. Information regarding rules of engagement.

j. Air and ground tactics of U.S./Allied/coalition forces.

k. Mishap/accident information of a privileged nature.

l. Association of call signs with unit designators.

PLANS

a. Changes in wartime mission/tasking.

b. Specific information of schedule of forces/equipment, staging locations.

c. Security classification of a classified operation, program, or project.

d. Intent to mobilize before public announcement.

e. Infrastructure reports.

f. Evacuation routes/procedures and rally points.

COMMUNICATIONS

a. Information revealing a COMSEC weakness (i.e., COMSEC, cybersecurity, TEMPEST, or physical security weaknesses).

b. Capabilities of communications equipment/system deficiencies—node(s), link(s), and impact.

c. Information revealing location of communications nodes or links (primary or alternate).

d. Communications system status, upgrades, or proposed changes.

e. Computer passwords, user IDs and/or network access paths.

INTELLIGENCE

a. Intelligence sources or methods of gaining intelligence; analytical methods and processes.

b. Intelligence assessments, maps, and location of intelligence targets.

LOGISTICS

a. Changes or shortages in equipment/command status that may impair mission capabilities.

b. New equipment capabilities/limitations.

c. Mass order/issue of specialized clothing.

BUDGET

a. Prioritization, preparation, and distribution of annual budget.

b. Increased/decreased budget costs of future force or mission changes.

c. Emergency requisition of funds that discloses details of contingency/wartime operations.

PERSONNEL

a. Personnel privacy issues/identifiers.

b. Identification and relation of command personnel with rating badge, security clearances/access, and special projects.

c. Immunization/medical requirements/health status and deficiencies.

d. Location, itineraries, and travel modes of key military and civilian personnel.

e. Manpower gains or losses associated with contingency operations or exercise.

f. Training deficiencies impairing mission accomplishment.

3. For questions about OPSEC or the contents of this memorandum, contact any member of the command OPSEC team.

C.1.2 Critical Information Value Matrix Worksheet

This step in the OPSEC process establishes the value of critical information based on its importance to both adversary and friendly objectives, and establishes subsequent impact to the organization or mission if that information is lost.

Mission Area/Subset	**CI Assessed Value**	
	Friendly	**Adversary**
MISSION AREA:		
Subset 1.		
Subset 2.		
etc.		
MISSION AREA:		
Subset 1.		
Subset 2.		
etc.		
MISSION AREA:		
Subset 1.		
Subset 2.		
etc.		
TOTALS		

Figure C-1. Critical Information Mission Area/Subset Value Matrix

Quantitative Values:	
HIGH:	5
MED-HI:	4
MEDIUM:	3
MED-LOW:	2
LOW:	1

Figure C-2. Quantitative Critical Information Values

Total Value Possible: NUMBER OF MISSION AREA LINES times 5=TOTAL VALUE POSSIBLE

OVERALL Assessed Friendly CI Value: SUM out of TOTAL POSSIBLE=RATING

OVERALL Assessed Adversary CI Value: SUM out of TOTAL POSSIBLE=RATING

C.1.3 Sample Critical Information Value Matrix Worksheet

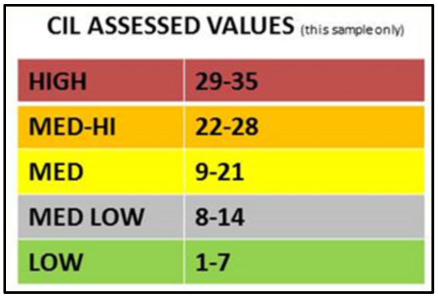
The following is a sample of a completed CI value matrix.

Mission Area/Subset	CI Assessed Value	
	Friendly	Adversary
MISSION AREA: COMMAND		
Subset 1. Mission times	5	5
Subset 2. Security Procedures	4	5
Subset 3. Aircrew home addresses	2	1
MISSION AREA: READINESS		
Subset 1. Supply and logistics levels	5	5
Subset 2. Budget information	3	2
MISSION AREA: C2		
Subset 1. IT infrastructure	5	4
Subset 2. Network diagrams	5	4
TOTALS	29/35	26/35

Figure C-3. Critical Information Mission Area/Subset Value Matrix Sample

Quantitative Values:	
HIGH:	5
MED-HI:	4
MEDIUM:	3
MED-LO:	2
LOW:	1

Figure C-4. Quantitative Critical Information Values



CIL ASSESSED VALUES (this sample only)

HIGH	29-35
MED-HI	22-28
MED	9-21
MED LOW	8-14
LOW	1-7

Figure C-5. CIL Assessed Values

Total Value Possible (in this sample only): 35

OVERALL Assessed Friendly Critical Information Value: 29 out of 35 or=HIGH rating

OVERALL Assessed Adversary Critical Information Value: 26 out of 35 or=MED-HI rating

In other words, we assess the loss of our critical information is HIGH and would have a severe impact on our ability to accomplish the mission if the adversary got their hands on it.

An adversary places a MED-HI value on our critical information, in order to achieve their objectives.

These ratings inform the commander of the relative value of their critical information to the unit and the adversary.

You will use these values when performing the risk analysis phase of the OPSEC process.

Critical Information Value Definition to Us (e.g., Unit, Installation)	Weighted Ranking	Critical Information Value Definition to Adversary	Weighted Ranking
HIGH: Loss of critical information (CI) will have a SEVERE impact on our ability to accomplish the mission.	5	HIGH: This CI is of CRITICAL importance to an adversary and obtaining the information CONSIDERABLY contributes to meeting adversary objectives.	5
MEDIUM HIGH: Loss of CI will probably have a SERIOUS impact on our ability to accomplish the mission.	4	MEDIUM HIGH: This CI is of CRUCIAL importance to an adversary and obtaining the information APPRECIABLY contributes to meeting adversary objectives.	4
MEDIUM: Loss of CI will likely have an APPRECIABLE impact on our ability to accomplish the mission.	3	MEDIUM: This CI is of ESSENTIAL importance to an adversary and obtaining the information GREATLY contributes to meeting adversary objectives.	3
MEDIUM LOW: Loss of CI will possibly have a MODERATE impact on our ability to accomplish the mission.	2	MEDIUM LOW: This CI is of MODERATE importance to an adversary and obtaining the information contributes to meeting adversary objectives.	2
LOW: Loss of CI could have a MINOR impact on our ability to accomplish the mission.	1	LOW: This CI is MINOR importance to an adversary.	1

Figure C-6. Critical Information Value Definitions Derived from DODM 5205.02-M

What we mean when we say:

Term	Meaning	Value
LIKELIHOOD	The probability of an event or situation taking place.	
CRITICAL	The existence of a vulnerability that could cause catastrophic, unrecoverable damage to the mission or operational effectiveness of the unit.	
CONSIDERABLY	Measurable risk term associated with impact or influence resulting in detrimental conditions of 90% or greater.	90–100%
SEVERE	The existence of a vulnerability that could cause exceptionally grave, but recoverable damage to the mission or operational effectiveness of the unit. Recovery time can exceed 96 hours.	
GREATLY	Measurable risk term associated with impact or influence resulting in detrimental conditions of 75% but less than 90%.	75–89%
SERIOUS	The existence of a vulnerability that could cause acute, recoverable damage to the mission or operational effectiveness of the unit. Recovery time can exceed 72 hours.	
SUFFICIENTLY	Measurable risk term associated with impact or influence resulting in detrimental conditions of 50% but less than 75%.	50–74%
APPRECIABLE	The existence of a vulnerability that could cause recoverable damage to the mission or operational effectiveness of the unit. Recovery time can exceed 48 hours.	
SIGNIFICANTLY	Measurable risk term associated with impact or influence resulting in detrimental conditions of 25% but less than 50%.	25–49%
MODERATE	The existence of a vulnerability that could cause nominal damage to the mission or operational effectiveness of the unit. Recovery time can exceed 24 hours.	
ESSENTIAL	Measurable risk term associated with impact or influence resulting in detrimental conditions of 10% but less than 25%.	10–24%
MINOR	The existence of a vulnerability that could cause nominal damage to the mission or operational effectiveness of the unit. Recovery time should not exceed 24 hours.	
USEFUL	Measurable risk term associated with impact or influence resulting in detrimental conditions of 10% or less.	10% or less

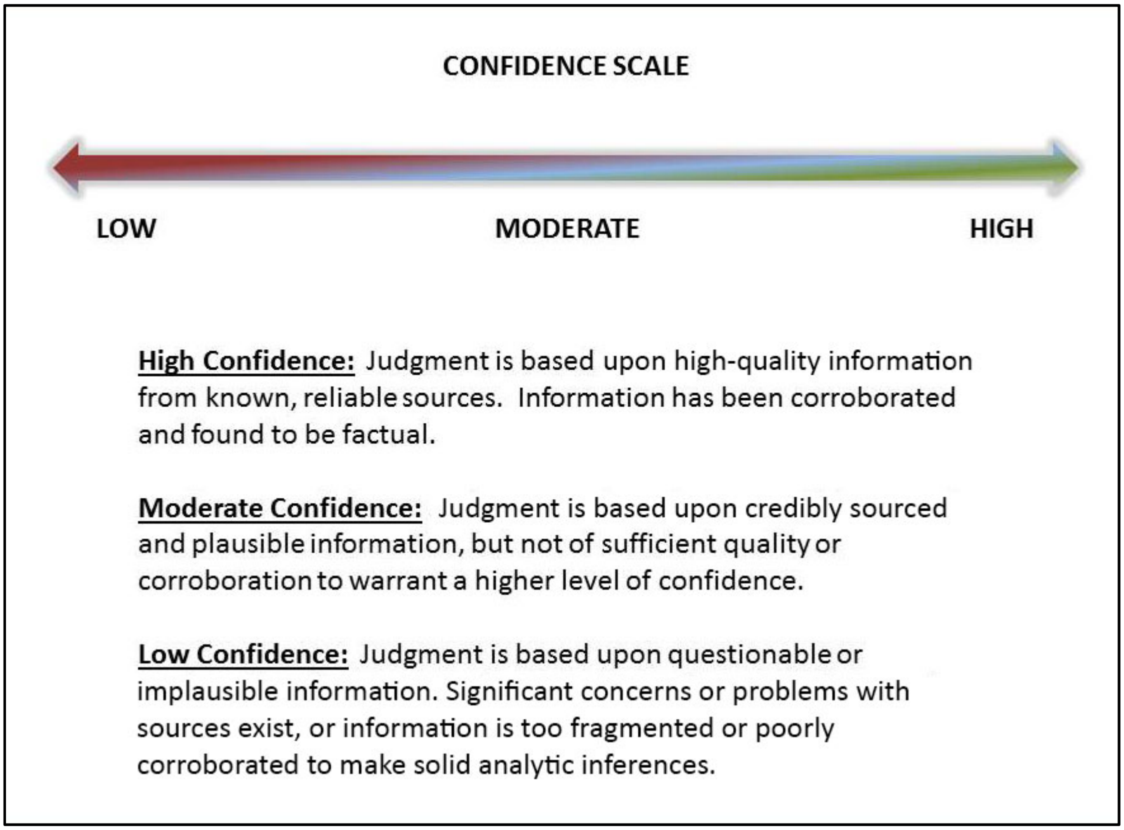
Figure C-7. Value and Terms Definitions

C.1.4 Sample Critical Information Value Assessment Summary and Confidence Statements

The following are recommended statements to accompany the critical information value assessment portion in the final OPSEC risk assessment.

[PARAGRAPH MARKING] Based on our interviews with [UNIT/ORGANIZATION NAME] personnel, and review of the [UNIT/ORGANIZATION NAME's] critical information list (CIL), combined with our assessment of adversarial interest in this information, we judge the [UNIT/ORGANIZATION NAME's] C2 mission area is of the highest importance to [UNIT/ORGANIZATION NAME] and adversaries alike. We judge mission area command is also assessed as being of high importance to both the [UNIT/ORGANIZATION NAME] and the adversary. Subsequent sections of this assessment address threat, vulnerabilities, and an overall risk analysis of the [UNIT/ORGANIZATION's] OPSEC posture.

(U) We have ______ confidence in the information derived from U.S. Government websites, documents, and reference materials, including all-source classified and unclassified resources. We have ______ confidence in the information derived from publicly available, open-source resources, including social media. We have ______ confidence in the information derived from corporate and/or corporate sponsored, publicly available resources, as this information is intended to influence as well as inform.



High Confidence: Judgment is based upon high-quality information from known, reliable sources. Information has been corroborated and found to be factual.

Moderate Confidence: Judgment is based upon credibly sourced and plausible information, but not of sufficient quality or corroboration to warrant a higher level of confidence.

Low Confidence: Judgment is based upon questionable or implausible information. Significant concerns or problems with sources exist, or information is too fragmented or poorly corroborated to make solid analytic inferences.

Figure C-8. Confidence Scale

INTENTIONALLY BLANK

APPENDIX D

OPSEC Input to an Information Operations Plan and Operations Order

D.1 OPLAN/OPORD: TAB C (OPERATIONS SECURITY) TO APPENDIX 3 (INFORMATION OPERATIONS) TO ANNEX C (OPERATIONS)

The following is a guide to writing the OPSEC input to an operations order, and should be mission-specific and distinct from the OPSEC program instruction. See JP 3-13.3, Operations Security.

Tab C—Operations Security

1. ( ) Situation. Refer to other annexes and paragraphs in the basic plan as much as possible to avoid duplication. When publishing the OPSEC annex separately from the basic order, it is necessary to copy the information here in detail. This allows the OPSEC annex to be a useful, stand-alone document. This section should also contain pertinent information from the intelligence preparation of the operational environment and the combined information overlay that helps inform OPSEC planning.

   a. ( ) Enemy forces.

      (1) ( ) Current enemy intelligence assessment. State the estimated enemy's assessment of friendly operations, capabilities, and intentions. Specifically, address any known enemy knowledge of the friendly operations covered in the basic plan.

      (2) ( ) Enemy intelligence capabilities. State the enemy's intelligence collection capabilities according to major categories (SIGINT, HUMINT, and so forth). Address all potential sources, to include the capabilities of any non-belligerents who may provide support to the enemy. Describe how the enemy's intelligence system works, to include the time required for intelligence to reach key decision makers. Identify major analytical organizations and key personalities. Discuss unofficial intelligence organizations, if any, that support the leadership. Identify strengths and weaknesses.

   b. ( ) Friendly forces.

      (1) ( ) Friendly operations. Briefly describe the major actions of friendly forces during execution of the basic plan.

      (2) ( ) Critical information. List the identified critical information. Include the critical information of higher headquarters. In phased operations, list critical information by phase; information that is critical in an early phase may not require protection in later phases.

   c. ( ) Assumptions. Identify any assumptions unique to OPSEC planning.

2. ( ) Mission. Provide a clear and concise statement of the OPSEC mission.

3. ( ) Execution.

   a. ( ) Concept of operations. Describe the general concept to implement OPSEC countermeasures. Give general concept description by phase, major activity, and how other IRCs will be integrated into the OPSEC plan. Address OPSEC support to other elements of the IO plan, if applicable.

b. ( ) Tasks. Identify specific OPSEC countermeasures that will be implemented. List by phase, if appropriate. Assign responsibility for execution to the command issuing the order or to subordinate commands. Add an exhibit to this tab for detailed or lengthy lists.

c. ( ) Coordinating instructions. Identify requirements to coordinate OPSEC countermeasures between subordinate elements. Address required coordination with public affairs. Provide guidance on how to terminate OPSEC related to activities of this operation. Address declassification and public release of OPSEC-related information. Describe OPSEC assessments conducted in support of this plan. Identify any after-action reporting requirements.

d. ( ) Feedback. Describe the concept for monitoring the effectiveness of OPSEC countermeasures during execution. Identify specific intelligence requirements for feedback. Commanders and their staffs can use feedback to adjust ongoing activities and for future OPSEC planning. Provisions for feedback should be coordinated with the command's intelligence and CI staffs to ensure requirements that support OPSEC receive the appropriate priority. Evaluate task accomplishment by assessing measures of effectiveness (doing the right things to achieve the objective) and measures of performance (Are things being done right?).

(1) ( ) Identifying these items while the plan is being developed will facilitate plan execution (MOP) (used to assess friendly accomplishment of tasks and mission execution) intelligence collection (MOEI), and assessment of the OPSEC plan's effectiveness (MOE).

(2) ( ) Identify specific MOP. Provides a way to determine if OPSEC countermeasures are being properly implemented.

Examples of Measures of Performance Feedback

- Numbers of populace listening to military information support operations (MISO) broadcasts
- Percentage of adversary command and control facilities attacked
- Number of civil-military operations projects initiated/number of projects completed
- Human intelligence reports number of MISO broadcasts during Commando Solo missions

(3) ( ) Assess the OPSEC plan's MOE. Monitor the adversary's reaction to determine the countermeasures' effectiveness in achieving the objective. Are desired effects achieved?

Possible Sources of Measures of Effectiveness Feedback

- Intelligence assessments (human intelligence, etc.)
- Open-source intelligence
- Internet (newsgroups, etc.)
- Military information support operations, and civil-military operations teams (face-to-face activities)
- Contact with the public
- Press inquiries and comments
- Department of State polls, reports, and surveys (reports)
- Open Source Center
- Nongovernmental organizations, intergovernmental organizations, international organizations, and host nation organizations
- Foreign policy advisor meetings
- Commercial polls
- Operational analysis cells

(4) ( ) Measure of effectiveness indicators. Add quantitative data points to qualitative MOEs, can assist the OPSEC staff or IO cell in answering questions related to a qualitative MOE, and can be identified from across the information environment.

Examples of Measures of Effectiveness Indicators

- A decrease in the number of anti-government rallies or demonstrations in a city since (a given timeframe); based on rallies/demonstrations observed.
- An increase in the percentage of positive new government media stories since (a given timeframe); based on media monitoring.
- An increase in the number of citizens participating in democratic functions since (a given timeframe); based on data or criteria such as voter registration, city council meeting attendance, and business license registration.
- An increase in the number of insurgents turned in or identified since (a given timeframe).

e. ( ) OPSEC assessments. Address any plans for conducting OPSEC assessments in support of the basic plan.

f. ( ) After-action reports. Identify any requirements for after-action reporting.

4. ( ) Administration and logistics. Give special OPSEC-related administrative or logistical support requirements.

5. ( ) Command and control.

a. ( ) Command relationships.

(1) ( ) Approval. State approval authority for execution and termination.

(2) ( ) Authority. Designate supported and supporting commanders as well as agencies, as applicable.

(3) ( ) Oversight. Detail oversight responsibilities, particularly for measures by nonorganic units or organizations outside of the chain of command.

b. ( ) Command, control, communications, and computer systems. Address any special or unusual OPSEC-related communications system requirements. List all communications system-related OPSEC countermeasures in paragraph 3.b.

APPENDIX E

Sample OPSEC Program Instruction

E.1 OPSEC PROGRAM INSTRUCTION

The following is a guide to writing an OPSEC program instruction that should be used to inform the OPSEC program for a unit, command, or activity. This should be general and outline the basis of conduct for the OPSEC program.

DEPARTMENT OF THE NAVY
COMMAND LETTERHEAD

Reference Information
Date

COMMAND INSTRUCTION NUMBER XXXX.X

Subj: OPERATIONS SECURITY (OPSEC)

Ref: (a) OPNAVINST 3432.1A
(b) JP 3-13.3
(c) DODD 5205.2e
(d) NTTP 3-13.3M

1. Purpose. To establish policy and provide guidance for implementing and managing [COMMAND NAME's] operations security (OPSEC) program.

2. Cancellation. [PRIOR INSTRUCTION]

3. Background. Information operations (IO) is the integrated employment, during military operations, of information-related capabilities (such as electronic warfare, military deception, and operations security) in concert with specified supporting and related capabilities, such as cyberspace operations and public affairs, to disrupt, corrupt, or usurp adversarial human and automated decision making while protecting our own. OPSEC supports, and is integrated with, the other information-related capabilities to deny an adversary the information needed for effective decision making and to focus and prioritize IO countermeasures to protect critical information.

a. OPSEC is not intended to be a replacement for traditional security programs that are designed to protect classified information. OPSEC is intended to deny adversaries publicly available indicators of sensitive or unclassified activities, capabilities, or intentions.

b. The potential for exploitation of open-source material, including Internet, media, and other generally unclassified but sensitive information, significantly challenging the ability to provide adequate force protection as well as the conduct of other sensitive or classified activities. As a result, OPSEC is vital in mitigating risks associated with all military operations.

c. References (a) through (d) provide doctrine and policy on OPSEC.

4. OPSEC Program.

a. OPSEC applies to all military functions at all levels of command. Therefore, a formal OPSEC program must be maintained with the goal of ensuring OPSEC practices are used to deny critical information to any potential adversary.

b. [COMMAND NAME] is actively involved in OPSEC, particularly in defining OPSEC goals and planning guidance, and in making decisions regarding the balance of operational and security needs.

c. All personnel reporting to [COMMAND NAME] are required to familiarize themselves with, and participate in, the command's OPSEC program. The OPSEC program manager will conduct annual assessments to determine the status of the OPSEC program, and take actions necessary to improve the program, as required by reference (a).

d. The OPSEC process is continuous, interactive, and described in detail in reference (d). The elements of the process are:

(1) Identification of critical information and its indicators.

(2) Analysis of threats.

(3) Analysis of vulnerabilities.

(4) Assessment of risks.

(5) Application of appropriate countermeasures.

5. Responsibilities.

a. OPSEC program manager. The OPSEC program manager is responsible for administering the OPSEC program per reference (d). The OPSEC program manager shall attend the Navy OPSEC Program Manager course (available through the NOST) or any relevant interagency courses (OPSE-2380, OPSE-2390) offered by the Interagency Operations Security Support Staff (IOSS). Every effort will be made to have department OPSEC assistants or working group members attend relevant courses. Other personnel in the command knowledgeable in areas that affect OPSEC will assist the OPSEC program manager in the execution of their duties. Additional duties of the OPSEC program manager include:

(1) Advising the commanding officer on all OPSEC matters

(2) Coordinating the development of the OPSEC-related portions of operations, plans, and orders

(3) Participating in IO planning, when applicable

(4) Developing and maintaining the command's OPSEC program, to include writing the organization's policy and guidance documents

(5) Conducting organizational OPSEC education and training

(6) Conducting the organization's annual OPSEC internal assessment per reference (a)

(7) Maintaining a compilation of OPSEC lessons learned

(8) Coordinating intelligence and CI support, as necessary

(9) Leading monthly OPSEC working group meetings to coordinate department action and support

(10) Advising external inspectors on the command's OPSEC program

(11) Coordinating OPSEC with traditional security program officers

(12) Coordinating with Navy Public Affairs and OPSEC program managers in support of reference (d)

(13) Integrating the OPSEC process into the planning and execution of applicable command operations (including routine operations, command Web sites, and all outgoing message traffic)

(14) Ensuring command personnel are informed of critical information and OPSEC measures are implemented to protect that critical information

(15) Providing guidance to public affairs officers for maintaining operations security.

b. OPSEC assistants or working group members. OPSEC assistants or working group member should be assigned from each department and assist the OPSEC program manager in their responsibilities. Additional duties include:

(1) Completing the IOSS OPSEC 1301 computer-based training

(2) Attending monthly OPSEC meetings and other meetings scheduled by the OPSEC program manager

(3) Being actively engaged in annual OPSEC assessments, awareness campaigns, and other OPSEC-related tasks as assigned

6. Training. All reporting personnel will receive an OPSEC orientation briefing during indoctrination sessions.

7. Continuing awareness. An effective OPSEC program requires constant attention by all hands. The OPSEC program manager will provide relevant reminders during all-hands calls and ensure that plan of the day(POD)/plan of the week (POW) notes regularly address OPSEC. Additionally, posters will be prominently displayed in workspaces and department. OPSEC working group members will make regular reports to department heads on their respective application of the OPSEC process.

8. Review responsibility. The OPSEC program manager will review this instruction annually.

C.O. SIGNATURE

INTENTIONALLY BLANK

APPENDIX F

Threat and Vulnerability Analysis

F.1 THREAT ANALYSIS

The following appendix is one of many methods that can be used to analyze OPSEC threats and vulnerabilities.

The threat assessment (TA) phase in the OPSEC process includes identifying potential adversaries in the operational environment and their associated capabilities, limitations, and intentions to collect, analyze, and use knowledge of our critical information against us. These ratings inform the commander of the threat value to their critical information. You will use these values when performing the risk analysis phase of the OPSEC process.

	Assessed Capability To Collect					
	ADVERSARY: (Name) Threat VECTOR: (HUMINT, SIGINT, GEOINT, MASINT, OSINT)	5—HIGH	4—MED-HIGH	3—MED	2—MED-LOW	1—LOW
Assessed Intent To Collect	5—HIGH					
	4—MED-HIGH					
	3—MED					
	2—MED-LOW					
	1—LOW					

Figure F-1. Threat Value Matrix

Capability Value Definitions:	Intent Value Definitions:
5—HIGH: The adversary's collection is highly developed and MOST LIKELY in place, or the adversary receives equivalent data collection support from a HIGHLY capable third party.	5—HIGH: The adversary is HIGHLY motivated and a successful outcome SIGNIFICANTLY contributes to meeting adversary objectives.
4—MEDIUM-HIGH (MED-HIGH): The adversary's collection capability is significantly developed and PROBABLY in place, or the adversary receives equivalent data collection support from a SIGNIFICANTLY capable third party.	4—MEDIUM-HIGH (MED-HIGH): The adversary is SIGNIFICANTLY motivated and a successful outcome GREATLY contributes to meeting adversary objectives.
3—MEDIUM: The adversary's collection capability is possibly developed and LIKELY in place, or the adversary receives equivalent data collection support from a CAPABLE third party.	3—MEDIUM: The adversary is SUFFICIENTLY motivated and a successful outcome WILL contribute to meeting adversary objectives.
2—MEDIUM-LOW (MED-LOW): The adversary's collection capability is probably not developed and MOST LIKELY NOT in place, or the adversary may receive equivalent data collection from a third party.	2—MEDIUM-LOW (MED-LOW): The adversary is MODERATELY motivated and a successful outcome CAN contribute to meeting adversary objectives.
1—LOW: The adversary collection capability is NOT developed, or does NOT receive data support from a third party.	1—LOW: The adversary is NOT motivated to collect information.

Figure F-2. Threat Value Definitions

What we mean when we say:

Term	Meaning
INTENT to Collect	Assessment of the adversary's intentions to collect, analyze, and use knowledge of our critical information against us. This assessment is based upon intelligence and all-source reporting, history, current events, political-military relations with the U.S., Allies, and adversaries, and knowledge of the adversary's technical and non-technical collection abilities.
CAPABILITY to Collect	Assessment of the adversary's ability to collect our critical information. Includes technical and non-technical means of collection. This assessment is based upon intelligence and all-source reporting, history, and knowledge of the adversary's technical and non-technical collection abilities. Typical OPSEC assessments include the following intelligence and information collection vectors: geospatial intelligence (GEOINT), human intelligence (HUMINT), measurement and signature intelligence (MASINT), open-source intelligence (OSINT), signals intelligence (SIGINT).
LIKELIHOOD	The probability of an event or situation taking place.
NOT	Opportunities may exist. However, there are no indications of interest, collection capability, or intent.
MODERATELY	Opportunities may exist. Adversary likely has interest but limited capability. No indications of intent or collection activity are present.
SUFFICIENTLY	Opportunities exist. Adversary has interest and collection capability. No indications of intent.
SIGNIFICANTLY	Opportunities exist. Adversary has interest and capability. Intent is present although no indications of specific current collection activity are underway.
HIGHLY	Opportunities exist. Adversary has interest and capability. Strong indications of intent. Confirmed indications of specific collection activity are underway.
CAN	Adversary is capable and opportunities exist. No indications of intent.
WILL	Adversary is capable, opportunities exist, and strong indications of intent are evident. Collection activity is either underway or imminent.

Figure F-3. Threat Terms and Definitions

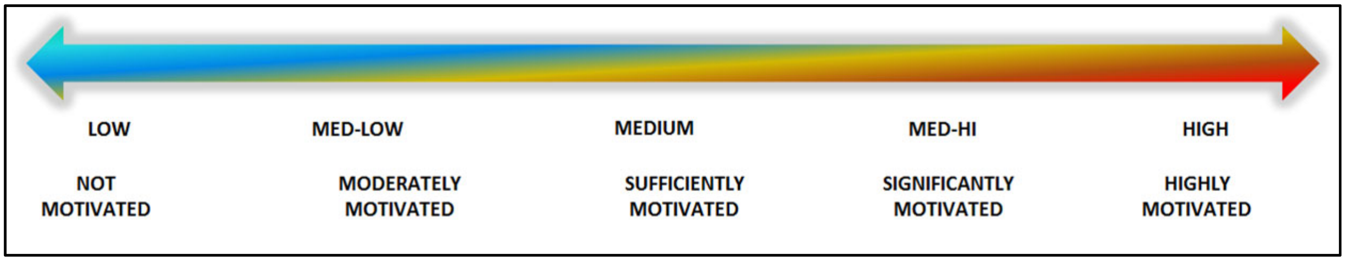


Figure F-4. Value Continuum

F.1.1 Sample Threat Value Matrix Worksheets

Notional values are assigned for illustration purposes.

		Assessed Capability To Collect				
	ADVERSARY (Name) Threat TYPE: HUMINT	5—HIGH	4—MED-HIGH	3—MED	2—MED-LOW	1—LOW
Assessed Intent To Collect	5—HIGH					
	4—MED-HIGH			12		
	3—MED					
	2—MED-LOW					
	1—LOW					

4 (intent)×3 (capability)=12

Figure F-5. Sample Threat Value 1

		Assessed Capability To Collect				
	ADVERSARY (Name) Threat TYPE: SIGINT	5—HIGH	4—MED-HIGH	3—MED	2—MED-LOW	1—LOW
Assessed Intent To Collect	5—HIGH					
	4—MED-HIGH					
	3—MED					
	2—MED-LOW		8			
	1—LOW					

2 (intent)×4 (capability)=8

Figure F-6. Sample Threat Value 2

	Assessed Capability To Collect					
	ADVERSARY (Name) Threat TYPE: GEOINT	5—HIGH	4—MED-HIGH	3—MED	2—MED-LOW	1—LOW
Assessed Intent To Collect	5—HIGH				10	
	4—MED-HIGH					
	3—MED					
	2—MED-LOW					
	1—LOW					

5 (intent)×2 (capability)=10

Figure F-7. Sample Threat Value 3

	Assessed Capability To Collect					
	ADVERSARY (Name) Threat TYPE: OSINT	5—HIGH	4—MED-HIGH	3—MED	2—MED-LOW	1—LOW
Assessed Intent To Collect	5—HIGH	25				
	4—MED-HIGH					
	3—MED					
	2—MED-LOW					
	1—LOW					

5 (intent)×5 (capability)=25

Figure F-8. Sample Threat Value 4

	Assessed Capability To Collect					
	ADVERSARY (Name) Threat TYPE: OSINT	5—HIGH	4—MED-HIGH	3—MED	2—MED-LOW	1—LOW
Assessed Intent To Collect	5—HIGH	25				
	4—MED-HIGH					
	3—MED					
	2—MED-LOW					
	1—LOW					

1 (intent)×1 (capability)=1

Figure F-9. Sample Threat Value 5

How to tally the scores:

Threat Assessment Table			
Threat Vector	Intent	Capability	Score
HUMINT	MED-HI	MED	12
SIGINT	MED-HI	MED-LOW	8
GEOINT	HIGH	MED-LOW	10
OSINT	HIGH	HIGH	25
MASINT	LOW	LOW	1
Overall Threat Value:			56 MEDIUM

Figure F-10. Threat Vulnerability Value Ranking

SUMMARY (of these samples only):

Total threat value possible per column: 25

That means: 5(intent)×5(capability)=25

Total threat value per assessment table=150

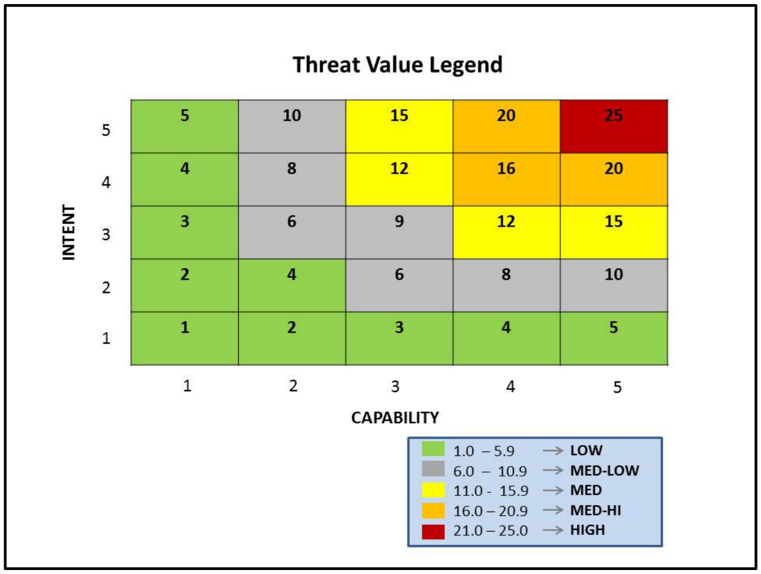
That means: 5 threat vectors times the max. threat value (25)=125

Overall threat score for this sample: 56 out of 125

Overall threat rating for this sample: MEDIUM

Overall Threat Value Ranking Scale	
Threat	Value
HIGH	101–125
MED-HI	76–100
MEDIUM	51–75
MED-LOW	26–50
LOW	1–25

Figure F-11. Overall Threat Value Ranking Scale



Threat Value Legend

INTENT					
5	5	10	15	20	25
4	4	8	12	16	20
3	3	6	9	12	15
2	2	4	6	8	10
1	1	2	3	4	5
	1	2	3	4	5
	CAPABILITY				

🟩	1.0 – 5.9	→ LOW
▨	6.0 – 10.9	→ MED-LOW
🟨	11.0 - 15.9	→ MED
🟧	16.0 – 20.9	→ MED-HI
🟥	21.0 – 25.0	→ HIGH

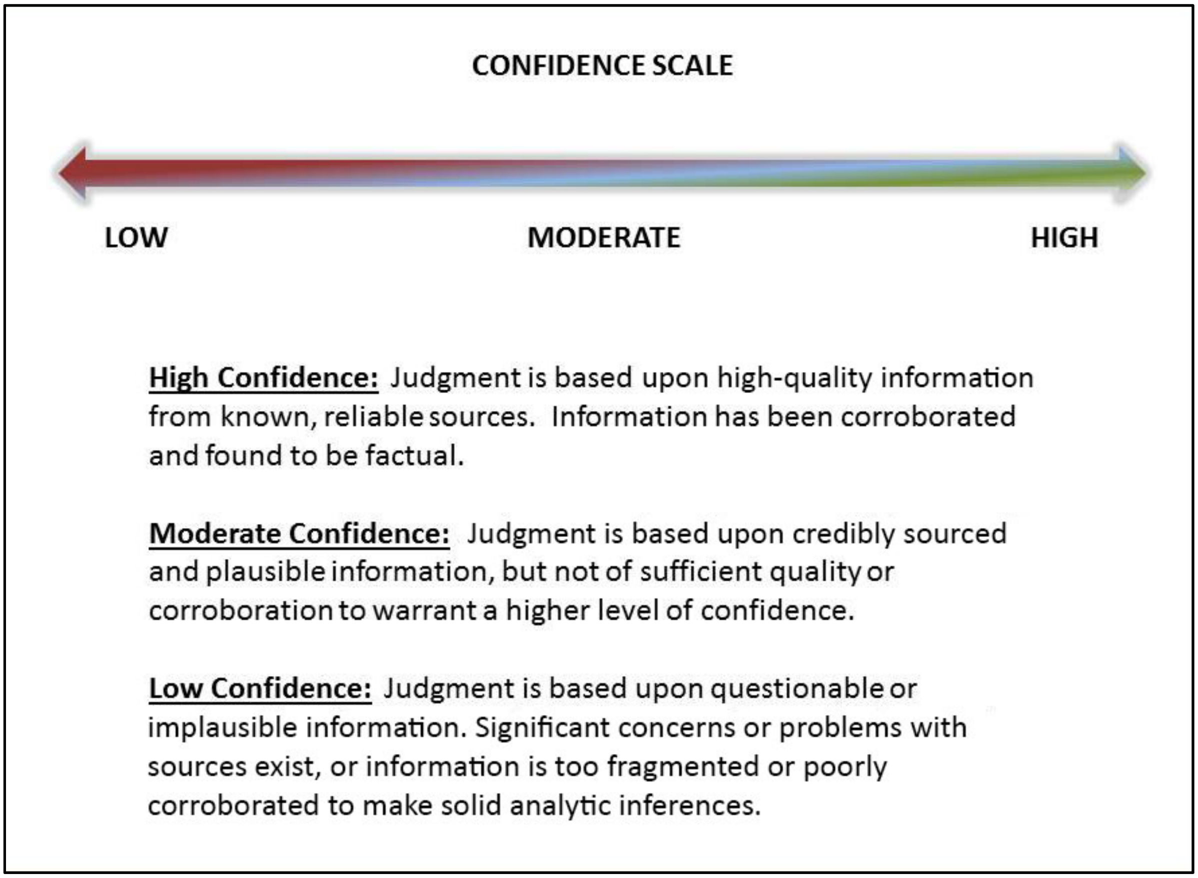
Figure F-12. Threat Value Legend

F.1.2 Sample Threat Assessment Summary and Confidence Statements

The following are recommended statements to accompany the threat assessment portion in the final OPSEC assessment.

[PARAGRAPH MARKING] Based on our examination of multiple adversarial intelligence and information collection vectors, open source intelligence (OSINT) collection activity by adversaries poses a HIGH threat to the [UNIT/ORGANIZATION NAME]. [HUMINT] collection activity by adversaries is assessed as posing a MEDIUM threat, while the remaining collection vectors are assessed as [MEDIUM-LOW or LOW threat]. See section ______ for recommended OPSEC measures and/or countermeasures to mitigate these threats.

(U) We have ______ confidence in information derived from U.S. Government websites, documents, and reference materials including all-source classified and unclassified resources. We have ______ confidence in information derived from publicly available, open source resources including social media. We have ______ confidence in information derived from corporate and/or corporate-sponsored, publicly available resources as this information is intended to influence as well as inform.



CONFIDENCE SCALE

High Confidence: Judgment is based upon high-quality information from known, reliable sources. Information has been corroborated and found to be factual.

Moderate Confidence: Judgment is based upon credibly sourced and plausible information, but not of sufficient quality or corroboration to warrant a higher level of confidence.

Low Confidence: Judgment is based upon questionable or implausible information. Significant concerns or problems with sources exist, or information is too fragmented or poorly corroborated to make solid analytic inferences.

Figure F-13. Confidence Scale

F.2 VULNERABILITY ANALYSIS

The vulnerability assessment (VA) phase in the OPSEC process measures the susceptibility of critical information to adversary collection. This step includes the identification of indicators that can also induce a susceptibility to adversary collection. These ratings inform the commander of the vulnerability value of losing their critical information to adversarial collection. You will use these values when performing the risk analysis phase of the OPSEC process.

Mission Areas	Assessed Vulnerability to Collection from Adversary					
		Collection Vector				
		HUMINT	SIGINT	OSINT	MASINT	GEOINT
	MISSION AREA:					
	Subset 1.					
	Subset 2.					
	etc.					
	MISSION AREA:					
	Subset 1.					
	Subset 2.					
	etc.					
	MISSION AREA:					
	Subset 1.					
	Subset 2.					
	etc.					
	TOTALS:					

Figure F-14. Vulnerability Analysis Worksheet

What we mean when we say**:**

Vulnerability Value Definitions
5—HIGH: Exploitation of this vulnerability by an adversary will make critical information susceptible to at least one intelligence collection discipline virtually any time the adversary chooses to collect.
4—MEDIUM-HIGH (MED HIGH): Exploitation of this vulnerability by an adversary will make critical information susceptible to at least one intelligence collection discipline most of the time the adversary chooses to collect.
3—MEDIUM: The adversary's capability to exploit this vulnerability is not well developed but could frequently make critical information susceptible to at least one intelligence collection discipline.
2—MEDIUM-LOW (MED LOW): The adversary's capability to exploit this vulnerability is poorly developed, and critical information is only occasionally susceptible to at least one intelligence collection discipline.
1—LOW: Potential for exploitation is negligible.

Figure F-15. Vulnerability Value Definitions

F.2.1 Sample Assessed Vulnerability to Collection from Adversary Matrix

(USING NOTIONAL VALUES IN EACH COLUMN.)

Mission Areas	Assessed Vulnerability To Collection From Adversary					
		Collection Vector				
		HUMINT	SIGINT	OSINT	MASINT	GEOINT
	MISSION AREA: COMMAND					
	Personnel rosters	3	1	2	1	1
	Command priorities	3	1	2	1	1
	MISSION AREA: READINESS					
	Training schedules	3	1	2	1	1
	Training rosters	3	2	2	1	1
	MISSION AREA: COMMUNICATIONS					
	Networks	1	5	1	1	3
	Infrastructure	1	5	1	1	2
	MISSION AREA: MOBILIZATION					
	Staging areas	3	3	3	3	5
	Ports of Departure	3	3	2	1	5
	TOTALS:	20	21	15	10	19

Figure F-16. Vulnerability Analysis Worksheet Sample

Total possible value per vector column (in this sample only): 40

Vulnerability Ranking Guide **By Individual Column** **(this sample only)**	
HIGH	31–40
MED-HI	25–31
MEDIUM	17–24
MED-LOW	9–16
LOW	1–8

Figure F-17. Vulnerability Ranking Guide

Threat Vector	Value	Vulnerability Rating
HUMINT	20/40	MEDIUM
SIGINT	21/40	MED-LOW
OSINT	15/40	MED-LOW
MASINT	10/40	MED-LOW
GEOINT	19/40	MEDIUM

Figure F-18. Threat Vulnerability Value Rating

How to tally the scores:

Vulnerability Assessment Table	
Collection Threat Vector	Score
HUMINT	20
SIGINT	21
OSINT	15
MASINT	10
GEOINT	19
Overall Threat Value:	85 MEDIUM

Figure F-19. Vulnerability Assessment Table

Overall Vulnerability Value Ranking Scale	
Vulnerability	Value
HIGH	160–200
MED-HI	121–160
MEDIUM	81–120
MED-LOW	41–80
LOW	1–40

Figure F-20. Overall Vulnerability Value Ranking Scale

Total possible value per vector column (in this sample only): 40

Total possible value of this worksheet (in this sample only): 200

That means: 40×5 columns=200

Overall vulnerability score (for this sample): 85 out of 200

Overall vulnerability rating (for this sample): MEDIUM

These ratings inform the commander of the relative vulnerability of losing their critical information to adversarial collection. You will use these values when performing the risk analysis phase of the OPSEC process.

F.2.2 Sample Threat Assessment Summary and Confidence Statements

The following are recommended statements to accompany the vulnerability assessment portion in the final OPSEC assessment (see figure F-13).

[PARAGRAPH MARKING] Based on our examination of the [UNIT/ORGANIZATION's] critical information, activities, personnel, and installation, we assess the [UNIT/ORGANIZATION] is most susceptible to adversarial collection activities from the [SIGINT] threat vector with an assessed [MEDIUM] vulnerability rating without OPSEC measures in place, (or without sufficient OPSEC measures in place). However, with implementation of sufficient OPSEC measures, we assess this vulnerability rating should fall to _______ after measures are applied and routinely monitored. See section _______ of this assessment for recommended countermeasures to mitigate vulnerabilities.

(U) We have _______ confidence in information derived from U.S. Government websites, documents, and reference materials including all-source classified and unclassified resources. We have _______ confidence in information derived from publicly available, open source resources including social media. We have _______ confidence in information derived from corporate and/or corporate sponsored, publicly available resources as this information is intended to influence as well as inform.

INTENTIONALLY BLANK

APPENDIX G

Risk Analysis and Countermeasure Considerations

G.1 RISK ANALYSIS CHARTS

G.1.1 Risk Assessment

The risk assessment phase of the OPSEC process combines determination of critical information with the findings and analysis of threats and vulnerabilities. The risk assessment is expressed as a measure of the probability that an adversary will be successful in collecting critical information and the resulting costs to the mission.

Probability is determined by multiplying a vulnerability value by the relative threat value. This worksheet contains the matrices for determining probability and impact based on specific threat vector (e.g., HUMINT, SIGINT, etc.) against identified vulnerabilities. It also contains a risk matrix worksheet for the combined risk value based upon all determined threats against all identified vulnerabilities.

G.1.2 OPSEC Risk Analysis Instructions

1. Critical Information

   a. Determine which items should reside on the unit or organization's critical information list (CIL).

   b. Using weighted ranking, assign numeric values of 1 to 5 (i.e., 1=LOW; 2=MED-LOW; 3=MED; 4=MED-HI; 5=HI) to each element in each mission area. These values are consistent with the qualitative levels of assessment cited in the DODM 5205.02-M.

See figure G-2.

2. Threat:

   a. Threat vectors cited in this risk model are derived from the DODM 5205.02-M, and include HUMINT, SIGINT, OSINT, GEOINT, and MASINT. Special consideration should be given to the SIGINT collection capabilities in the cyber domain.

   b. Determine adversary threat vectors based upon intent and capability.

   c. The numeric value for threat is determined by multiplying the value assessed for intent by the value assessed for capability (threat=intent×capability). Although we could cite other elements (e.g., opportunity, targeting, history, etc.), we only cite intent and capability in this risk model to be consistent with the DODM 5205.02-M.

   d. Similar to the weighted ranking of critical information, this risk formula evaluates threat on a scale of five possible values (e.g., 1=LOW, 2=MED-LOW, 3=MED, 4=MED-HI, 5=HIGH).

   e. Assign a numeric value to each of these qualitative values, then multiply across.

See figures G-5 through G-9.

3. Vulnerability:

   a. Using the mission areas from the CIL, assess vulnerabilities of each mission area subset to adversarial collection from each of the five adversarial collection vectors (e.g., HUMINT, SIGINT, OSINT, MASINT, GEOINT).

   b. Assign numeric values of 1 to 5 to each specific mission area item as they appear vulnerable to adversary collection by the five collection vectors.

   c. Only the highest vulnerability value to the overall mission area are cited in the risk assessment matrix worksheet.

See figure G-13.

4. Risk assessment:

   a. To achieve a quantitative value for assessing the risk of adversarial collection of critical information, a combination of previously completed assessment factors are blended and tallied in the risk assessment phase of the OPSEC process. The risk assessment matrix worksheet contains unit and organization critical information, which is divided into functional mission areas. Each subset of each mission area contains a numeric value depicting its value or importance to the unit or organization.

   b. Using the data from the critical information matrix worksheet, enter the value for the mission area subset in the columns for each of the threat vectors. This value remains constant when factored against each adversarial threat collection vector because we value the item regardless of the threat.

   c. Using the data from the threat value matrix worksheet, enter the value of the assessed threat from each of the five threat vectors.

   d. Using the data from the vulnerability matrix worksheet, enter the value of the assessed vulnerability to adversarial collection.

   e. The risk score is the sum of the critical information value times the threat value times the vulnerability value (risk=CI×threat×vulnerability).

See figure G-18.

G.2 RISK ASSESSMENT

Mission Area: Command	**Threat Vector**				
	HUMINT	SIGINT	OSINT	MASINT	GEOINT
Subset 1.					
Threat Value					
Vulnerability Value					
RISK SCORE					
Subset 2.					
Threat Value					
Vulnerability Value					
RISK SCORE					
Mission Area: Readiness	**Threat Vector**				
	HUMINT	SIGINT	OSINT	MASINT	GEOINT
Subset 1.					
Threat Value					
Vulnerability Value					
RISK SCORE					

Figure G-1. Risk Assessment Matrix Worksheet

G.3 SAMPLE COMPLETED WORKSHEETS

The following sample worksheets (with notional values assigned for illustration purposes) are provided as a model for compiling phases one through four of the OPSEC risk analysis process. The final phase, OPSEC measures, will be addressed in a separate document.

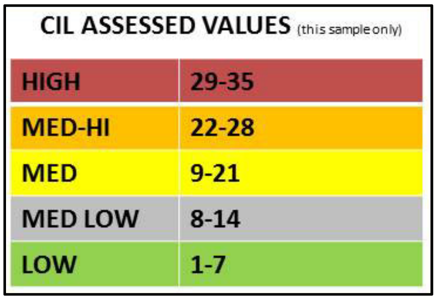
G.3.1 Critical Information Value Matrix

Mission Area/Subset	CI Assessed Value	
	Friendly	Adversary
MISSION AREA: Command		
Subset 1. Mission times	5	5
Subset 2. Security Procedures	4	5
Subset 3. Aircrew home addresses	2	1
Mission Area: Readiness		
Subset 1. Supply and logistics levels	5	5
Subset 2. Budget information	3	2
Mission Area: C2		
Subset 1. IT infrastructure	5	4
Subset 2. Network diagrams	5	4
TOTALS:	29/35	26/35

Figure G-2. Critical Information Mission Area and Subset Value Matrix Sample

Quantitative Values:	
HIGH:	5
MED-HI:	4
MEDIUM:	3
MED-LOW:	2
LOW:	1

Figure G-3. Quantitative Critical Information Values



CIL ASSESSED VALUES (this sample only)	
HIGH	29-35
MED-HI	22-28
MED	9-21
MED LOW	8-14
LOW	1-7

Figure G-4. CIL Assessed Values

Total value possible (in this sample only): 35

OVERALL Assessed Friendly Critical Information Value: 29 out of 35 or=HIGH rating

OVERALL Assessed Adversary Critical Information Value: 26 out of 35 or=MED-HI rating

In other words, we assess the risk of loss of our critical information is HIGH and would have a severe impact on our ability to accomplish the mission if the adversary got their hands on it.

An adversary places a MED-HI value on our critical information, in order to achieve their objectives.

These ratings inform the commander of the relative value of their critical information to the unit and the adversary.

You will use these values when performing the risk analysis phase of the OPSEC process.

G.3.2 Threat Value Matrix

	Assessed Capability To Collect					
	ADVERSARY (Name) Threat TYPE: HUMINT	5—HIGH	4–MED-HIGH	3—MED	2—MED-LOW	1—LOW
Assessed Intent To Collect	5—HIGH					
	4—MED-HIGH			12		
	3—MED					
	2—MED-LOW					
	1—LOW					

Figure G-5. Sample Completed Threat Value 1

	Assessed Capability To Collect					
	ADVERSARY (Name) Threat TYPE: SIGINT	5—HIGH	4–MED-HIGH	3—MED	2—MED-LOW	1—LOW
Assessed Intent To Collect	5—HIGH					
	4—MED-HIGH					
	3—MED					
	2—MED-LOW		8			
	1—LOW					

Figure G-6. Sample Completed Threat Value 2

	Assessed Capability To Collect					
	ADVERSARY (Name) Threat TYPE: GEOINT	5—HIGH	4–MED-HIGH	3—MED	2—MED-LOW	1—LOW
Assessed Intent To Collect	5—HIGH				10	
	4—MED-HIGH					
	3—MED					
	2—MED-LOW					
	1—LOW					

Figure G-7. Sample Completed Threat Value 3

	Assessed Capability To Collect					
	ADVERSARY (Name) Threat TYPE: OSINT	5—HIGH	4—MED-HIGH	3—MED	2—MED-LOW	1—LOW
Assessed Intent To Collect	5—HIGH	25				
	4—MED-HIGH					
	3—MED					
	2—MED-LOW					
	1—LOW					

Figure G-8. Sample Completed Threat Value 4

	Assessed Capability To Collect					
	ADVERSARY (Name) Threat TYPE: MASINT	5—HIGH	4—MED-HIGH	3—MED	2—MED-LOW	1—LOW
Assessed Intent To Collect	5—HIGH					
	4—MED-HIGH					
	3—MED					
	2—MED-LOW					
	1—LOW					1

Figure G-9. Sample Completed Threat Value 5

How to tally the scores:

Threat Assessment Table			
Threat Vector	Intent	Capability	Score
HUMINT	MED-HI	MED	12
SIGINT	MED-HI	MED-LOW	8
GEOINT	HIGH	MED-LOW	10
OSINT	HIGH	HIGH	25
MASINT	LOW	LOW	1
Overall Threat Value:			56 MEDIUM

Figure G-10. Threat Vulnerability Value Ranking

Summary (of this sample only):

Total threat value possible per column: 25

That means: 5×5=25

Total threat value per assessment table=150

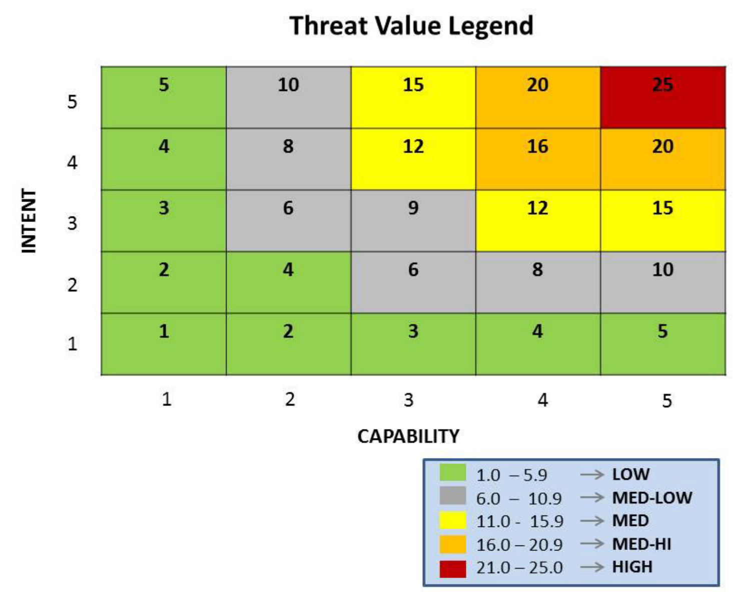
That means: 5 threat vectors times the max. threat value (25)=125

Overall threat score for this sample: 56 out of 125

Overall threat rating for this sample: MEDIUM

Overall Threat Value Ranking Scale	
Threat	Value
HIGH	101–125
MED-HI	76–100
MEDIUM	51–75
MED-LOW	26–50
LOW	1–25

Figure G-11. Overall Threat Value Ranking Scale



Threat Value Legend

INTENT

5	5	10	15	20	25
4	4	8	12	16	20
3	3	6	9	12	15
2	2	4	6	8	10
1	1	2	3	4	5
	1	2	3	4	5

CAPABILITY

🟩	1.0 – 5.9	→	LOW
⬜	6.0 – 10.9	→	MED-LOW
🟨	11.0 - 15.9	→	MED
🟧	16.0 – 20.9	→	MED-HI
🟥	21.0 – 25.0	→	HIGH

Figure G-12. Threat Value Legend

G.3.3 Vulnerability Value Matrix

Mission Areas	Assessed Vulnerability to Collection from Adversary					
		Collection Vector				
		HUMINT	SIGINT	OSINT	MASINT	GEOINT
	MISSION AREA: COMMAND					
	Personnel rosters	3	1	2	1	1
	Command priorities	3	1	2	1	1
	MISSION AREA: READINESS					
	Training schedules	3	1	2	1	1
	Training rosters	3	2	2	1	1
	MISSION AREA: COMMUNICATIONS					
	Networks	1	5	1	1	3
	Infrastructure	1	5	1	1	2
	MISSION AREA: MOBILIZATION					
	Staging areas	3	3	3	3	5
	Ports of Departure	3	3	2	1	5
	TOTALS:	20	21	15	10	19

Figure G-13. Completed Vulnerability Value Matrix Sample

Total possible value per vector column (in this sample only): 40

Vulnerability Ranking Guide By Individual Column (this sample only)	
HIGH	31–40
MED-HI	25–31
MEDIUM	17–24
MED-LOW	9–16
LOW	1–8

Figure G-14. Vulnerability Ranking Guide

Threat Vector	Value	Vulnerability Rating
HUMINT	20/40	MEDIUM
SIGINT	21/40	MED-LOW
OSINT	15/40	MED-LOW
MASINT	10/40	MED-LOW
GEOINT	19/40	MEDIUM

Figure G-15. Threat Vulnerability Value Rating

How to tally the scores:

Vulnerability Assessment Table	
Collection Threat Vector	Score
HUMINT	20
SIGINT	21
OSINT	15
MASINT	10
GEOINT	19
Overall Threat Value:	85 MEDIUM

Figure G-16. Sample Vulnerability Assessment Table

Overall Vulnerability Value Ranking Scale	
Vulnerability	Value
HIGH	160–200
MED-HI	121–160
MEDIUM	81–120
MED-LOW	41–80
LOW	1–40

Figure G-17. Overall Vulnerability Value Ranking Scale

Total possible value per vector column (in this sample only): 40

Total possible value of this worksheet (in this sample only): 200

That means: 40×5 columns=200

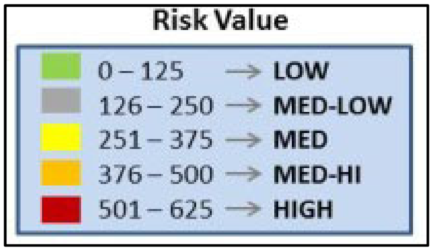
Overall vulnerability score (for this sample): 85 out of 200

Overall vulnerability rating (for this sample): MEDIUM

G.3.4 Risk Assessment Matrix

CIL: Mission Area—Command	**Threat Vector**				
	HUMINT	**SIGINT**	**OSINT**	**MASINT**	**GEOINT**
CIL Subset 1. Mission Times	5	5	5	5	5
Threat Value	12	12	9	1	4
Vulnerability Value	3	1	2	1	1
RISK SCORE	180	60	90	5	20
CIL Subset 2. Security Procedures	4	4	4	4	4
Threat Value	12	12	9	1	4
Vulnerability Value	3	1	3	1	1
RISK SCORE	144	48	108	4	16
CIL: Mission Area—Readiness	**Threat Vector**				
	HUMINT	**SIGINT**	**OSINT**	**MASINT**	**GEOINT**
CIL Subset 1. Personnel (medical, training, DRRS, etc.)	5	5	5	5	5
Threat Value	12	8	12	1	10
Vulnerability Value	3	1	4	1	1
RISK SCORE	180	40	240	5	50
CIL Subset 2. Budget	3	3	3	3	3
Threat Value	10	8	14	1	1
Vulnerability Value	3	1	4	1	1
RISK SCORE	90	32	168	3	3
TOTAL RISK	594/2500 = MED-LOW	180/2500 = LOW	606/2500 = MED-LOW	17/2500 = LOW	89/2500 = LOW

Figure G-18. Risk Matrix Worksheet Sample



Risk Value

🟩	0 – 125	→ LOW
▨	126 – 250	→ MED-LOW
🟨	251 – 375	→ MED
🟧	376 – 500	→ MED-HI
🟥	501 – 625	→ HIGH

Figure G-19. Risk Value

OPSEC risk formula: CIL (subset)×THREAT×VULNERABILITY=RISK SCORE

Summary: In this notional scenario, the total possible value per threat vector column equals 2,500 points.

For example, the total amount of points that can be accumulated for the HUMINT column is 2,500; the same for SIGINT, OSINT, and so on because each CIL subset, threat, and vulnerability can only total 625 points using the following formula: CIL (subset) times threat times vulnerability equals risk score.

That is: 5 (highest score for critical information)×5 (highest score for vulnerability)×25 (highest score for threat)=625.

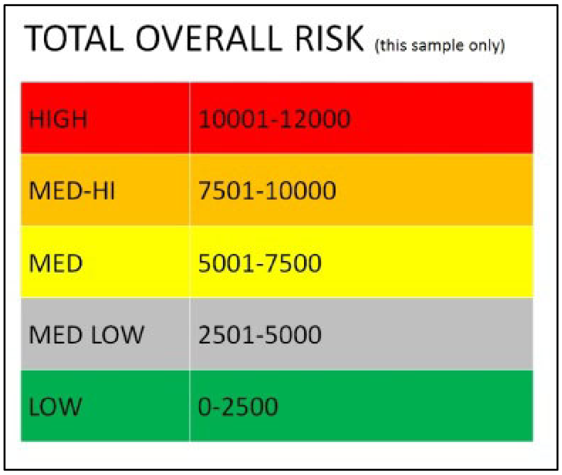
625×4=2,500—because we are only assessing 4 CIL items in this sample worksheet.

Tally all totals to determine the overall risk level.

In this case, 2,500×5=12,500. Total values of each column equals 2,314, which equates to a LOW rating →

If you were to brief the commander on these findings, you would say something like:

“Based on available reporting and information, and using this risk analysis formula, the risk to the unit’s critical information from HUMINT collection is assessed as MED-LOW; LOW from SIGINT; MED-LOW from OSINT; and LOW from MASINT and GEOINT collection. Combined, the overall risk level is LOW, based upon these findings.”



TOTAL OVERALL RISK (this sample only)

HIGH	10001-12000
MED-HI	7501-10000
MED	5001-7500
MED LOW	2501-5000
LOW	0-2500

Figure G-20. Total Overall Risk

G.4 COUNTERMEASURE CONSIDERATION

Phase four of risk analysis is identifying and applying OPSEC measures.

1. OPSEC measures, including action control measures, countermeasures, and counteranalysis, are designed to prevent an adversary from detecting critical information, to provide an alternative interpretation of critical information or indicators (deception), or to deny the adversary's collection system. If the amount of risk is determined to be unacceptable, countermeasures are then implemented to mitigate risk or to establish an acceptable level. Countermeasures should be coordinated and integrated with other information operations core capabilities, if applicable.

2. There are many best practices for countermeasures throughout the Department of Defense. Organizations may consult with OPSEC practitioners, security specialists, information technology specialists, and organizations with similar missions. However, countermeasures should not be regarded as risk-avoidance measures to be pulled from a list and implemented. Prior to recommending countermeasures, commanders or directors must carefully consider cost and their potential to degrade mission accomplishment.

3. Action control measures are internal actions to eliminate the unit's unique indicators or vulnerabilities. Examples of action control measures include:

   a. Using secure communication equipment such as STU-III, STE, S-VOIP, etc.

   b. Applying appropriate markings to information destined for dissemination

   c. Trash control, e.g., 100 percent shred policy

   d. Disseminating the unit CIL to all members of the unit

   e. Performing OPSEC training and briefings.

4. OPSEC countermeasures are designed to disrupt effective adversary collection. Examples of OPSEC countermeasures include:

   a. Electronic jamming (counters SIGINT collection)

   b. Leveraging police, e.g., powers-of-arrest (counters HUMINT collection)

   c. Coordinating activities with counterintelligence assets (counters HUMINT collection)

   d. Physical attack or destruction.

5. OPSEC counteranalysis prevents accurate interpretations of what an adversary is able to see or observe about the unit. Examples of OPSEC counter analysis measures include:

   a. Deceptions and ruses.

   b. Cover and camouflage.

   c. Use of decoys.

   d. Truth projections through press or news releases.

   e. Military information support operations (MISO).

Implementation of OPSEC Measures will aid in reducing the unit's vulnerabilities to adversarial collection and mitigate the amount and usefulness of unit-related information an adversary can use to their advantage.

G.5 COUNTERMEASURE CONSIDERATIONS

1. What is the cost versus benefit?
2. Do we really need it?
3. Are we creating a new vulnerability?
4. Are we creating new indicators?
5. What is the impact on operations?
6. How long is it needed?
7. How will we measure effectiveness?
8. Have we addressed all vulnerabilities with unacceptable risks?
9. Does this countermeasure reduce the risk to an acceptable level?
10. Does this countermeasure reduce the risk of more than one vulnerability?
11. Are there indicators that need separate countermeasures?
12. Will the culture accept the countermeasure and use it?
13. Will the leadership support the implementation of this countermeasure?
14. Is this the simplest solution?
15. Have we fully coordinated?

INTENTIONALLY BLANK

APPENDIX H

OPSEC Assessment Team Composition and Responsibilities

H.1 TEAM COMPOSITION

The size and composition of an OPSEC assessment team determine the scope of the assessment. Members of the team come from all divisions and departments, and should be thoroughly qualified in their functional areas and obtain OPSEC training. The assessment team ideally consists of a team leader and team members with expertise in the following function areas (mission and resource dependent):

1. Operations
2. Physical Security
3. Computer Network Operations
4. Administration
5. Supply or Logistics
6. Maintenance
7. Communications
8. Foreign Disclosure
9. Legal Officer
10. Public Affairs Officer
11. Network Security
12. Intelligence
13. Plans
14. Ombudsman or Family Readiness Officer
15. Contracting Support Team
16. Information Management or Assurance
17. Webmaster or Web Administrator
18. Information Operations.

H.2 TEAM MEMBER RESPONSIBILITIES

The following are general responsibilities of the team.

1. Team leader

   a. Briefs team members at their initial meeting, covering at a minimum:

      (1) Organization and purpose of the OPSEC assessment team.

      (2) How the team will conduct the assessment.

      (3) How the team will process the results of the assessment.

      (4) A list of directives and other applicable documents.

   b. Organizes, coordinates, directs assessment activity (to include interviews), and prepares the OPSEC assessment report.

   c. Meets with and supervises team members to assess progress, guide and assist, compare data, identify significant deficiencies, and consolidate reports and recommend actions.

   d. Correlates and analyzes information acquired by individual team members and through empirical studies (e.g., COMSEC, noncommunications monitoring, etc.); develop recommendations to reduce or eliminate OPSEC weaknesses.

   e. Provides briefs and comments to correct minor items on the spot in order to increase OPSEC awareness during the assessment.

   f. Provides the CO or OIC a verbal completion brief or report, followed by a final, written OPSEC assessment report.

2. Team members

   a. Develop EEFIs, the critical information list, and other relevant profiles in their respective functional areas.

   b. Acquire information to identify OPSEC vulnerabilities by means of observation, interview, and other data collection techniques.

   c. Are familiar with other team members’ functional areas and are alert for information that may affect them.

   d. Conduct interviews and consolidate results.

   e. Assist the team leader in preparing the final OPSEC assessment brief or report.

APPENDIX I

Disclosure Guidance for Command and Unit Movements

I.1 COMMAND AND UNIT MOVEMENTS

This appendix highlights the fact that there is no single approach to protecting information. Clearly, information marked confidential or above should be handled in accordance with procedures outlined in appropriate classification guides, orders, or this appendix. All personnel need to review those procedures to ensure no inadvertent release of information occurs. The fact remains that the vast majority of information we deal with on a daily basis is unclassified. The important point is that much of this unclassified information should still be considered sensitive and for official use only. It is in these areas that personnel are to be more vigilant in assessing their role in the disclosure of such information. There certainly is information that must be shared to do our jobs, but we must exercise sound judgment and, when in doubt, ask the chain of command for guidance.

As the naval forces conduct the business of training, equipping, and deploying our forces around the world to combat terrorism, a review of classification and disclosure policies is warranted prior to the release of any information, in order to ensure that the information that supports these critical operations is properly safeguarded. Merely classifying information cannot guarantee such safeguards. The strongest protection available is the proper disclosure of both classified and sensitive unclassified information only to those individuals with appropriate clearance and a need to know.

The following are examples of information classified at least confidential and should be disclosed only to authorized individuals.

1. Discussion of ongoing or future operations to include details of specific combat missions, battle damage assessments, force movements, and employment schedules.

2. Precise current location of forward deployed units (i.e., latitude and longitude).

The following are examples of unclassified information, some of which may be sensitive. The decision to release this information should only be made after a risk assessment on the effects such a disclosure would have on the forces involved (using the five-step OPSEC process) is completed.

1. Disclosure of a specific date 48 hours in advance of arrival or departure of individual units to or from U.S. bases. While disclosure prior to this time may be necessary to support maintenance, logistics, and PA, this disclosure shall be kept to the minimum required for the coordination of unit arrival or departure.

2. Disclosure of a specific date 7 days in advance of a unit’s return from or departure to deployment. The advance disclosure timeframe (7 days vice 48 hours) is in the recognition of the inherent logistics support and intense family interest in the movements of a combat unit. As discussed above, disclosure prior to this time should be limited and evaluated based on the risk such disclosure may have on the units involved.

For further information on classifying information see OPNAVINST S5510.XX series of instructions.

INTENTIONALLY BLANK

APPENDIX J

Contracts

J.1 OVERVIEW

OPSEC must be included in contracts in order to ensure that critical information is protected. Divulging this information to the adversary could potentially affect mission success and cause harm to military members, civilians, and contractors and their families. Below is an example of how to include OPSEC into contracts.

J.2 CONTRACT LANGUAGE EXAMPLE

1.1 Operations Security

Background, OPSEC is a process used to protect unclassified sensitive information from exploitation by an adversary. Sensitive unclassified information—which is also referred to as critical information or critical program information (CPI)—is defined as information that is not classified but which needs to be protected from unauthorized disclosure. Examples are information labeled "For Official Use Only (FOUO)," proprietary information, contractor sensitive information, limited distribution information, and personally identifiable information (PII).

1.1.1

The contractor and all subcontractors shall provide OPSEC protection for sensitive unclassified information as identified in the critical information list and CPI list, if applicable. The prime contractor and all subcontractors shall employ the countermeasures listed below in order to protect that information. Additional countermeasures may be employed as necessary. If an OPSEC Plan is provided, the contractor and all subcontractors shall comply with that plan. These OPSEC requirements will be in effect throughout the life of the procurement from award through the conclusion of services at the end of the period of performance (PoP) or other procurement termination. If required, the contractor and all subcontractors shall prepare an OPSEC Plan.

1.1.2

Contractor personnel shall follow OPSEC concepts and principles in the conduct of this requirement to protect critical information, personnel, facilities, equipment, and operations from compromise. The contractor shall consult with the subject matter expert (SME) within 5 working days of receipt of order to determine all special circumstances affecting OPSEC under this requirement. In any case where there is uncertainty or ambiguity regarding OPSEC measures, the contractor shall consult the SME as soon as possible. If the SME is unavailable, the contractor shall consult the contracting officer. The prime contractor and all subcontractors shall provide OPSEC protection for sensitive unclassified information and comply with all OPSEC requirements.

1.1.3 Minimum Protection Requirements for Critical Information

Critical information is exempt from public release under Exemption 2 of the Freedom of Information Act (FOIA). It is designated "For Official Use Only (FOUO)" and is considered controlled unclassified information (CUI). Specific CPI, for reasons of OPSEC will not be identified to offerors prior to award. CPI will be identified to the successful offeror only after receipt of contract award.

1.2 Personally Identifiable Information (PII)

PII shall be protected in accordance with DOD and Navy directives, in such a manner as to prevent unauthorized disclosure. Email containing PII must be encrypted or password protected.

1.3 Controlled Unclassified Information (CUI)

CUI is official information that requires the application of controls and protective measures for a variety of reasons and has not been approved for public release, to include technical information, proprietary data, information requiring protection under the Privacy Act of 1974, and Government-developed privileged information involving the award of contracts. CUI is a categorical designation that refers to unclassified information that does not meet the standards for National Security Classification under Executive Order(s), but is pertinent to the national interest of the United States or to the important interests of entities outside the Federal Government, and under law or policy requires protection from unauthorized disclosure, special handling safeguards, or prescribed limits on exchange or dissemination.

1.3.1 Minimum Requirements for Access to CUI

Prior to access, contractor personnel requiring access to DON CUI or “user level access to DON or DOD networks and information systems, system security and network defense systems, or to system resources providing visual access and/or ability to input, delete or otherwise manipulate sensitive information without controls to identify and deny sensitive information” who do not have clearance eligibility are required to submit a Questionnaire for Public Trust Positions (Standard Form 85P) through the cognizant Facility Security Officer or contractor entity representative for a suitability determination by DON Central Adjudication Facility.

1.3.2 Minimum Protection Requirements for CUI

Contract deliverables taking the form of unclassified limited-distribution documents (FOUO), are not authorized for public release and therefore shall not be posted on a publicly accessible Web server, nor electronically transmitted via electronic mail unless appropriately encrypted or password protected.

1.4 Countermeasures

Countermeasures are required to negate the susceptibility of critical information to exploitation by an adversary or competitor. The contractor shall protect all critical information listed in a manner appropriate to the nature of the information, including use of the necessary countermeasures as listed below applicable to specific items:

1. Encryption with a password of electronically stored critical information.

2. Encryption or password protection of e-mail containing critical information.

3. Storage of hard copy critical information, optical media, and external hard drives in locked containers when not in use.

4. Transmission of critical information to the minimum set of recipients with a need to know.

5. Proper marking of critical information with warnings to include at a minimum “FOR OFFICIAL USE ONLY”; as appropriate to the nature of the critical information it shall also be marked with “UNCLASSIFIED BUT SENSITIVE,” “PRIVACY ACT INFORMATION,” “PERSONALLY IDENTIFYING INFORMATION,” “PROTECT FROM UNAUTHORIZED DISCLOSURE,” or other similar statements cautioning protection of the critical information.

6. Restricting disclosure of critical information at meetings and conferences (including teleconferences) to the minimum necessary to the performance of this requirement.

7. Immediate and appropriate destruction in a manner precluding reconstruction of all critical information no longer needed under this requirement.

8. Restricting verbal discussion of critical information to venues and circumstances that prevent the monitoring and interception of the discussion by unauthorized personnel.

9. Maintaining current, successful completion of Navy-mandated information assurance (IA) and OPSEC training by all personnel handling critical information.

10. Refraining from the use of unencrypted telephones to transmit critical information.

11. Refraining from the use of foreign postal systems to ship critical information.

12. Promptly retrieving documents containing critical information printed on printers accessible by persons without a need to know the critical information.

13. Use of cover pages or other appropriate means to prevent the viewing of critical information by unauthorized persons.

14. Limiting the inclusion of critical information in contract and budget documents, presentations, press releases, and other publications to that which is essential to the performance of this requirement.

15. Use of protected databases and strong passwords and the protection of user identifications (User IDs).

16. During test and evaluation events (as applicable to this requirement) practice OPSEC methodologies with respect to staging units, personnel, and materials out of the observation of unauthorized persons; desensitization; and the speed of execution of the event.

1.5 Compromise

The contractor shall notify the SME, FSO, and security office immediately of all known and suspected compromises of critical information, classified information, or PII. If the SME cannot be reached, the contractor shall notify the contracting officer (or the command duty officer if after normal work hours).

1.6 FOUO

The FOUO marking is assigned to information at the time of its creation. It is not authorized as a substitute for a security classification marking but is used on official Government information that may be withheld from the public under exemptions 2 through 9 of the Freedom of Information Act (FOIA). Use of FOUO markings does not mean that the information can’t be released to the public, only that it must be reviewed by the Government prior to its release to determine whether a significant and legitimate government purpose is served by withholding the information or portions of it.

1.6.1

All UNCLASSIFIED documents created under this contract that contain FOUO information will be marked “FOR OFFICIAL USE ONLY” on the bottom of the cover page and interior pages.

1.6.2

Classified documents containing FOUO do not require any markings on the cover of the document. However, the interior pages containing only FOUO information shall be marked at the top and bottom center with “FOR OFFICIAL USE ONLY.” Only unclassified portions containing FOUO shall be marked with “(FOUO)” immediately before each unclassified FOUO portion.

1.6.3

All FOUO information released to the contractor will be marked with the following statement prior to transfer:

THIS DOCUMENT CONTAINS INFORMATION EXEMPT FROM MANDATORY DISCLOSURE UNDER THE FOIA. EXEMPTIONS(S) ______ APPLY.

1.6.4

Removal of the FOUO marking may be accomplished only by the originator or other competent authority. The contractor shall not remove any FOUO marking without written authorization from corona or the author. The Government will notify the contractor when the FOUO status is terminated.

1.6.5

The contractor is authorized to disseminate FOUO information to its employees and those having a need to know the information in order to accomplish the requirements of the contract.

1.6.6

When in use, reasonable steps shall be taken to minimize the risk of access to FOUO information by unauthorized personnel. FOUO information shall be placed in an out-of-sight location if the work area is accessible to persons who do not have a need to know the information in order to perform contract requirements. When not in use, the FOUO information shall be stored in a locked desk, file cabinet, bookcase, rooms, or other lockable container or space affording reasonable protection from unauthorized disclosure.

1.6.7

FOUO information may be delivered via U.S. Postal Service first-class mail, parcel post, and fourth-class mail for bulk shipments only. The contractor shall not permit FOUO information to enter foreign postal systems and parcel delivery systems.

1.6.8

When no longer needed, FOUO information shall either be returned to appropriate Government custody or destroyed in a manner precluding reconstruction of the information.

1.6.9

Electronic transmission of FOUO information (via voice, data, or facsimile transmission) shall be by approved secure communications systems or if transmitted over non-secure means, encryption or password protected documents must be used. If circumstances preclude the use of such a system, the contractor shall consult the SME; if the SME is not available and time requirements do not permit delay, the contractor shall consult the contracting officer.

1.6.10 Access Briefings

FSO will provide any necessary access briefings required for contract performance (NATO, etc.).

1.6.11

Classified information performance will occur only at locations specified in the DD254.

1.7 Additional Contract Language for OPSEC Requirements

Consideration should be given to include the following Defense Federal Acquisition Regulation (DFAR) clauses for all service support contracts: DFARS 252.227-7020; 252.204.7000; 252.204.7003; 252.204.7008; 252.204.7009; 252.204.7012.

1.7.1 Government Furnished Training

The Government will provide, or provide contractor access to all mandated Information Assurance (IA) and Cyber Awareness training required in support of this contract to allow establishment of Government IT user accounts and access to Government operated networks. All other training requirements required to attain, or maintain skill levels and qualifications of contractor personnel are considered contractor responsibility and will not be reimbursed by the Government.

1.7.2 Security Requirements

Personnel who are not cleared in accordance with these requirements will not be granted access to the designated Government facilities and cannot perform work in support of this PWS. Detailed security requirements shall be in accordance with DOD Contract Security Classification Specification (DD254).

1.7.3

The contractor and its personnel shall not divulge any information about files, data, processing activities or functions, user IDs, passwords or other knowledge that may be gained to anyone who is not authorized to have access to such information. Further, such conduct may be cause for criminal prosecution and imposition of severe criminal and civil penalties.

1.7.4

The Contractor and all associated employees shall not disclose sensitive information obtained as a result of working this contract, to include the personal identity of personnel working in support of this mission. This includes names, addresses and other contact information.

1.7.5

The contractor and all associated subcontractor employees shall comply with applicable local area policies and guidance for access security procedures provided by the U.S. Government. In addition to the changes otherwise authorized by the changes clause of this contract, should the force protection condition (FPCON) at any individual facility, installation or location change, the U.S. Government may require changes in contractor security matters or processes.

1.7.6

The contractor will ensure contractor employee comply with established Command OPSEC policy to protect the Government’s critical information in accordance with MCO 3070.2A, the Marine Corps Operations Security (OPSEC) Program. This also requires new contractor employees to complete Welcome Aboard training and all contractor employees must complete annual OPSEC awareness training. All contractor employees shall complete DOD information assurance awareness training and OPSEC training before issuance of network access and annually thereafter. All contractor employees working IA/IT functions must comply with DOD and Marine Corps training requirements in DODD 8570.01, DOD 8570.01-M, within 6 months after being employed.

1.7.7 Loss or Suspension of Security Facility Clearance

The Government reserves the right to direct contractor employees to be removed from work, directly or indirectly, whenever there is probable cause to believe that such action is warranted in the interest of national security. This action shall be made whether or not the cause is deemed of sufficient severity to warrant action to terminate the contractor’s Facility Clearance or individual’s security clearance. The Government also reserves the right to remove any contractor for the purpose of conducting any investigation of alleged misconduct which may, in the opinion of the Contracting Officer, jeopardize the security of the project.

1.7.8 Public Release Statement

Any information (classified and unclassified) pertaining to this contract shall not be released for public dissemination except as provided by the Industrial Security Manual or unless it has been approved for public release by appropriate U.S. Government authority. Proposed public release shall be submitted for approval at least 10 working days (or as directed by the hiring activity) prior to release/disclosure. In the case of non-DOD user agency, requests for disclosure shall be submitted to that agency at least 15 working days prior to requested release date.

APPENDIX K

Web Site Self-Assessment Checklist

K.1 OVERVIEW

Commands are encouraged to use self-assessment checklists to ensure that critical information is absent from public viewing. Conducting an internal assessment is an annual requirement, but each time the Web page is updated with new or additional information, it should be reviewed for content. The Navy Web Risk Assessment Cell at NETWARCOM developed the following Web site self-assessment checklist that is a vital tool geared for publicly accessible Navy Web sites.

K.2 NAVY AND MARINE CORPS PUBLICLY ACCESSIBLE WEB SITES

This document contains a summary of Web site content requirements and restrictions for publicly accessible Navy and Marine Corps Web sites, as set forth in SECNAVINST 5720.44C. A Web site satisfies the definition of being "publicly accessible" if any of the content on the Web site is accessible by the public via anonymous access. Restricting access by domain validation or secure socket link without client-side authentication is not sufficient to be excluded from the definition of "publicly accessible."

1. The following are rules governing authorized publicly accessible Web presences:

   a. No entity below the command level or its equivalent is authorized to establish a publicly accessible Web site.

   b. Only commissioned units are authorized to register a domain name for a Web site. Subordinate commands are allowed to create a Web presence, but only as a sub-Web of an authorized Web site. Sub-Webs will appear as an integral part of their command level parent Web site. For instance, sub-Webs will be implemented with the same "theme" as the parent Web site and any "home" buttons on the sub-Web pages must only link to the parent's Web site home page.

2. Navy and Marine Corps publicly accessible Web sites must:

   a. Contain the command's full organizational name.

      (1) The full command organizational name (with no abbreviations) must be prominently displayed on the Web site home page.

      (2) Contain the statement, "This is an official U.S. Navy Web site" or "This is an official U.S. Marine Corps Web site." The exact phrase, "This is an official U.S. Navy (Marine Corps) Web site" must be prominently displayed on the Web site home page. The Privacy and Security Notice must be verbatim from DOD Web site Administration Policies and Procedures, DOD INST 8550.01. The only authorized modifications are to substitute the command's organizational name in the places indicated. Figure K-1 shows a sample privacy and security notice.

   b. Contain the Webmaster information. Information on how to contact the Webmaster must be displayed on the Web site home page or at least contained within the source code of the home page. Ideally, Webmaster contact information should be listed on the Web site home page and should include an e-mail address, work telephone number, and work mailing address.

PRIVACY AND SECURITY NOTICE

1. [Name of service (e.g., “Website Title”)] is provided as a public service by [name of the DOD Component(s)].

2. Information presented on this service not identified as protected by copyright is considered public information and may be distributed or copied. Use of appropriate byline, photo, and image credits is requested.

3. For site management, information is collected [Link “information is collected” to description of specific information. An example is provided after paragraph 8. in this figure] for statistical purposes. This U.S. Government computer system uses software programs to create summary statistics, which are used for such purposes as assessing what information is of most and least interest, determining technical design specifications, and identifying system performance or problem areas.

4. For site security purposes and to ensure that this service remains available to all users, software programs are employed to monitor network traffic to identify unauthorized attempts to upload or change information, or otherwise cause damage.

5. Except for authorized law enforcement investigations and national security purposes, no other attempts are made to identify individual users or their usage habits beyond DOD Web sites. Raw data logs are used for no other purposes and are scheduled for regular destruction in accordance with National Archives and Records Administration Guidelines. [Agencies subject to Reference (o) shall add the following sentence to this paragraph: “All data collection activities are in strict accordance with DOD Directive 5240.01.”]

6. Web measurement and customization technologies (WMCT) may be used on this site to remember your online interactions, to conduct measurement and analysis of usage, or to customize your experience. The Department of Defense does not use the information associated with WMCT to track individual user activity on the Internet outside of Defense Department Web sites, nor does it share the data obtained through such technologies, without your explicit consent, with other departments or agencies. The Department of Defense does not keep a database of information obtained from the use of WMCT. [If the DOD CIO has provided explicit written approval to use Tier III WMCT, cite that approval here.] General instructions for how you may opt out of some of the most commonly used WMCT is available at http://www.usa.gov/optout_instructions.shtml.

7. Unauthorized attempts to upload information or change information on this site are strictly prohibited and may be punishable under the Computer Fraud and Abuse Act of 1987 and the National Information Infrastructure Protection Act (18 U.S.C. § 1030).

8. If you have any questions or comments about the information presented here, please forward them to [contact information to report both technical and information problems with the Web site specifically, including accessibility problems].

Figure K-1. Privacy and Security Notice

c. Contain a link to parent command or ISIC.

d. Contain a link to the official U.S. Navy Web site: http://www.navy.mil or http://www.usmc.mil.

e. Contain a link to the Navy recruiting Web site: http://www.navy.com or http://www.marines.com.

f. External links to non-U.S. Government Web sites shall be accompanied by a disclaimer statement.

(1) External links to non-Government Web sites that directly support the command’s mission are authorized, but a disclaimer statement must be displayed on the page or pages listing external links or through an intermediate “exit notice” page.

(2) External link disclaimer notice—Examples:

"The appearance of external hyperlinks does not constitute endorsement by the United States Department of Defense, the United States Department of the Navy and [command name] of the linked Web sites, or the information, products or services contained therein. For other than authorized activities such as military exchanges and Morale, Welfare and Recreation sites, the United States Department of Defense, the Department of the Navy and [command name] does not exercise any editorial control over the information that may be found at these locations. Such links are provided consistent with the stated purpose of the DOD Web site."

"The appearance of hyperlinks does not constitute endorsement by the [insert sponsoring organization, e.g., Department of Defense, U.S. Army, U.S. Navy, U.S. Air Force, or U.S. Marine Corps] of non-U.S. Government sites or the information, products, or services contained therein. Although the [insert sponsoring organization] may or may not use these sites as additional distribution channels for Department of Defense information, it does not exercise editorial control over all of the information that you may find at these locations. Such links are provided consistent with the stated purpose of this Web site."

g. All solicitations from the Web site visitor shall be accompanied by a privacy advisory.

The term "solicitation" encompasses any and all requests for submissions including surveys, forms and Webmaster feedback. An example of a privacy advisory is:

"We will not obtain personally identifying information about you when you visit our site unless you choose to provide such information to us. If you choose to send e-mail to the site Webmaster or submit an online feedback form, any contact information that you provide will be solely used to respond to your request and not stored."

h. Have the written approval of the Secretary of Defense for the use of persistent cookies. A cookie that is set to expire greater than 24 hours after being set is considered to be "persistent."

i. All session cookies and preapproved persistent cookies must be accompanied by a disclosure statement. The disclosure statement must state: that the site contains a cookie, why the cookie is being used, and the safeguards in place to protect any information collected.

j. A Notice and Consent Banner. A verbatim Notice and Consent Banner (sometimes referred to as a DOD Warning Banner) must be prominently displayed at the access point for Web sites where access is controlled by a level of security and access control mechanism (i.e., user authentication). The banner can be found at: http://iase.disa.mil/Pages/index.aspx.

Notice and Consent Banner Notice—example:

You are accessing a United States Government (USG) information system (IS) that is provided for USG-authorized use only.

By using this IS (which includes any device attached to this IS), you consent to the following conditions:

- The USG routinely intercepts and monitors communications on this IS for purposes including, but not limited to, penetration testing, COMSEC monitoring, network operations and defense, personnel misconduct (PM), law enforcement (LE), and counterintelligence (CI) investigations.

- At any time, the USG may inspect and seize data stored on this IS.

- Communications using, or data stored on, this IS are not private, are subject to routine monitoring, interception, and search, and may be disclosed or used for any USG-authorized purpose.

- This IS includes security measures (e.g., authentication and access controls) to protect USG interests—not for your personal benefit or privacy.

- Notwithstanding the above, using this IS does not constitute consent to PM, LE, or CI investigative searching or monitoring of the content of privileged communications, or work product, related to personal representation or services by attorneys, psychotherapists, or clergy, and their assistants. Such communications and work product are private and confidential. See User Agreement for details.

k. Contain a link to Freedom of Information Act (FOIA) Web site: http://www.foia.navy.mil.

l. Contain a link to Suicide Prevention Lifeline Web site: https://www.veteranscrisisline.net/. It must be linked through the Veterans Crisis Line logo found on the page.

m. Contain a link to No Fear Act: http://www.secnav.navy.mil/donhr/Site/Pages/No-Fear-Act.aspx

n. Ensure all photos have been assigned a visual information record identification number (VIRIN) and are properly archived. To learn what a VIRIN is, visit http://www.dimoc.mil/.

o. Web sites must include a Section 508 link on the Web site: http://dodcio.defense.gov/dodsection508/std_stmt.aspx

p. U.S. Navy and Marine Corps publicly accessible Web sites must NOT contain:

(1) Overt warning signs or words of warning or danger in association with the Privacy Policy. The Privacy Policy can only be identified with the phrase "Privacy Policy." Indicators that create a misperception of danger in association with the Privacy Policy will not be used. The Privacy Policy can only be identified with the phrase "Privacy Policy."

(2) Altered photos (other than standard photographic processes). Some alterations are acceptable as long as the alterations do not defer from the original intent.

(3) FOUO or above information. Guidance for FOUO information is contained in DOD 5400.7R.

(4) Personally identifying content, i.e., any information that can be used to identify DOD individuals. The exception is command executives (i.e., CO, XO, CMC) can be identified by photo and name only. The following specific information is not to be divulged:

(a) Social Security Number

(b) Family Members

(c) Home Address or Phone Numbers

(d) Birth Date or Place

Figure K-2. Veterans Crisis Line Logo

(e) Race, Religion, Citizenship

(f) City Home of Record

(g) Marital Status

(h) Personalized E-mail Address

(i) Age.

(5) Proprietary or copyrighted content.

(6) Operational lessons learned.

(7) Information revealing sensitive military operations, exercises, vulnerabilities, maps identifying command, and operational facilities.

(8) Information for a specialized, internal audience or of questionable value to the general public that is not access-limited by, at least, password protection and client-side authentication. Only content specifically targeted for the general public should be posted on Web sites that have no access restrictions implemented. Content intended for an internal audience will, at a minimum, have access limited by password protection, in addition to client-side authentication.

(9) Information that places national security, personnel, assets, or mission effectiveness at unacceptable risk.

(10) Phone numbers that can be associated with individuals. Only phone numbers for commonly requested resources and services or for office codes are allowed.

(11) Product endorsement, preferential treatment of any private organization or product, or references, including logo or text indicating that the site is "best viewed" with any specific Web browsers.

(12) Contain links or references to documents within DOD Web sites that have security and access controls. However, it is permissible to link to log-on sites, provided details as to the controlled site's contents are not revisited.

(13) Content duplicated from other military Web resources.

Note

Navy Web sites may reference (via hyperlink) these external resources instead. For example, you may provide a link to: http://www.navy.mil/navydata/fact.asp for ship characteristics.

K.3 SAMPLE WEBSITE REVIEW FORM

(unit name) OFFICIAL WEBSITE REVIEW - xx QTR/FYxx

United States Marine Corps organizations' websites hosted on the Internet will be examined using a comprehensive OPSEC Review Checklist and will be reviewed for OPSEC compliance at least quarterly.

Operations Security (OPSEC). OPSEC is a process of identifying critical information and subsequently analyzing friendly actions attendant to defense acquisitions, military operations, and other activities in order to: i) identify those actions that can be observed by adversary intelligence systems; and ii) determine what indicators might be obtained by hostile intelligence systems that could be interpreted or pieced together to derive critical information in time to be useful to adversaries; and iii) select and execute measures that eliminate or reduce risk, to the vulnerabilities of friendly actions to adversary exploitation, to an acceptable level.

Unclassified Websites. Unclassified, publicly available websites present a potential risk to personnel, resources, system development, and operations, if inappropriate information is published on websites. OPSEC program manages and coordinators will ensure their command's website(s) are reviewed to ensure there is no critical information published via text, graphics, or photographs.

OPSEC Review Checklist for Official Websites

Organization's Name:

References: *DODM 5205.02-M, SECNAVINST 3070.2, MCTP 3-32B, and MCO 3070.2A*

Reviewer's Name:	Date/Time of Website Review:
Organization Reviewed:	Primary Website Address/URL:

Issue/Concern:	***Yes***	***No***	***Notes/Comments:***
Website Content Requirements and Restrictions (See Note 1): **<u>I. Requirements.</u>** 1. Is the website registered? All official Marine websites (e.g., official websites and/or social media sites) must be registered at http://www.marines.mil/Units/Site-Registration/.			

Issue/Concern:	*Yes*	*No*	*Notes/Comments:*
2. Does the website contain the organization’s name and mailing address?			
3. Does the website contain a Privacy Policy or a hyperlink to the Privacy Policy on the website homepage?			
4. Does the website have the statement, “This is an official U.S. Marine Corps website?”			
5. Does the website contain a link to the official U.S. Marine Corps website: www.marines.mil?			
6. Does the website contain a disclaimer statement for external links to non-governmental websites, if applicable? (Example: DISCLAIMER: *This is an official U.S. Marine Corps page. However, the appearance of hyperlinks does not constitute endorsements by the U.S. Marine Corps. The U.S. Marine Corps does not exercise any editorial control over the information you may find at linked locations.)*			
7. Does the website contain a Notice and Consent Banner or DOD Warning Banner for consent to monitoring?			
8. Does the website have written approval for the use of persistent cookies?			
9. Do all session cookies and pre-approved persistent cookies have a disclosure statement?			

Issue/Concern:	*Yes*	*No*	*Notes/Comments:*
10. Does the website contain the Webmaster contact information displayed on the homepage or within the source code of the homepage? 11. Does the website contain a link to Freedom of Information Act (FOIA) website: http://www.hqmc.marines.mil/Agencies/USMC-FOIA? 12. Does the website contain a link to No Fear Act for DOD? 13. Does the website contain an Accessibility (DOD Section 508) link for all U.S. citizens, including persons with disabilities? 14. Websites may display biographies of general officers, commanders, commanding officers, officers in command, executive officers or deputies, the civilian equivalents, and Master Gunnery Sergeants or Sergeants Major. a. Websites may contain biographies about Marine/NCO/Civ of the month/quarter/year bios, or other recognition, e.g., awards, reenlistments, promotions, special achievements, etc. may be acceptable.			

Issue/Concern:	*Yes*	*No*	*Notes/Comments:*
b. General telephone numbers, non-personalized e-mail addresses for commonly-requested resources, services, and contacts, without individuals' names, are permitted. c. The names, telephone numbers, and official e-mail addresses of command/activity public affairs personnel and/or those designated by the commander as command spokespersons are also allowed. **II. Restrictions.** 1. Does the website(s) contain altered photos (other than standard photographic processes)? 2. Are all photos assigned a Visual Information Record Identification Number (VIRIN)? Are they properly archived? 3. Website cannot contain FOUO or above information. 4. Does personally identifiable information (PII) appear in any information posted to the website? For example, ● Social Security Account Numbers ● Dates of Birth ● Home Addresses ● Home Telephone Numbers ● Information that violates other privacy programs, e.g. HIPAA, Privacy Act 5. Does the website contain proprietary or copyrighted content?			

Issue/Concern:	*Yes*	*No*	*Notes/Comments:*
6. Does the website contain information indicating plans and Operational Lessons Learned that would reveal sensitive military operations, exercises, vulnerabilities, or maps identifying command and operational facilities? 7. Does the website contain any technical data (**See Note 2**) such as: ● Weapon Schematics ● Weapon System Vulnerabilities ● Electronic Wire Diagrams ● Frequency Spectrum Data 8. Does the website display information that could place national security, personnel, assets, or mission effectiveness at risk? 9. Does the website contain phone numbers that identify an individual other than those addressed in 14.c. above? Only phone numbers for commonly requested resources and services are allowed. 10. Does the website contain product endorsements, give any indication of preferential treatment of any private organization or product, or reference any logo or text indicating that the site is “best viewed” with any specific web browsers? 11. Does the website contain classified material, sensitive but unclassified information, controlled unclassified information, or information that could enable the recipient to infer this type of information?			

Issue/Concern:	*Yes*	*No*	*Notes/Comments:*
12. Does the website contain operations orders, threat condition profiles, or information relating to ongoing criminal investigations? 13. Does the website display force protection levels, specific force protection measures, or number of involved personnel? 14. Does the website display battle rhythm events, TTPs, Plans of the Day, Plans of the Month, and Research Development Test & Evaluation (RDT&E) data? 15. Does the website identify family members of U.S. Marine Corps personnel (military or civilian), and spouses of senior leadership participating in public events such as commissioning, ship naming, and family member information will not be included in any online biographies? a. Biographies cannot include date of birth, current residential location, nor any information about family members when displayed on official website(s). 16. Does the website contain personnel lists/rosters, organizational charts, or command staff directories which contain individuals’ name, phone numbers, or e-mail addresses?			

Issue/Concern:	*Yes*	*No*	*Notes/Comments:*
OPSEC Considerations: **“Indicators” (See Note 3):** Does the website contain relevant information in the following categories that might reveal an organizations plans and intentions? 1. Administrative: ● Personnel Travel (personal and official business). ● Attendance at planning conferences. ● Commercial support contracts. ● Family support plans. 2. Operations, Plans, and Training: ● Operations orders and plans. ● Mission specific training. ● Exercise and simulations activity. ● Exercise, deployment, or training schedules. ● Unit relocation/deployment. ● Inspection results, findings, deficiencies. ● Unit vulnerabilities or weaknesses. 3. Communications: ● RF emissions and associated documentation. ● Changes in activity or communications patterns. ● Availability of secure communications. ● Bulletin board/messages between Marines and family members.			

Issue/Concern:	***Yes***	***No***	***Notes/Comments:***
4. Logistics/Maintenance: ● Supply and equipment orders/deliveries. ● Transportation plans. ● Mapping, imagery, and special documentation support. ● Maintenance and logistics requirements. ● Receipt or installation of special equipment.			
Sensitive and Critical Information (Essential Secrets) "Key Word" Search: Use the Command-approved critical information list (CIL) to complete a "key word" search of documents found in public domain. The following are examples of key words that may be searched using available search engines: ● Deployment Schedules ● Exercise Plans ● Contingency Plans ● Training Schedules ● Inspection results, findings, deficiencies ● Biographies ● Family Support Activities ● Phone Directories, Lists ● Plans and lessons learned ● Personal Information (SSN, DOB, Home address/phone, identifying information on family members ● Technical data (schematics, IT vulnerabilities) ● General Officer Itinerary			

- NOTES -

Note 1: This checklist contains a summary of website content requirements and restrictions for publicly available U.S Marine Corps websites. A website satisfies the definition of being "publicly accessible" if any of the content on the website is accessible by the public via anonymous access. **Reference:** Website Self-Assessment Checklist, updated, 03 March 2015.

Note 2: Technical data creates a unique challenge to the OPSEC posture of an organization and to National Security as a whole. Certain technical data, when compiled with other unclassified information, may reveal an additional association or relationship that meets the standards for classification under
Reference: E.O. 12958, Section 1.8 (e).

Note 3: OPSEC Indicators are friendly detectable actions and open source information that can be interpreted or pieced together by an adversary to derive critical information.

By necessity this list is generic in nature. There are many other indictors possible for the wide range of military operations and activities. While this list is rather large—when placed in the context of commands ***pre-established*** critical information, this list may then be applied with a greater level of accuracy. This checklist is not a panacea for complete organization's OPSEC program. If an organization has not invested the effort to analyze its own critical information, then this list may only tend to exacerbate the problem.

Within the context of information assurance, the World Wide Web should not be treated any differently from any other potential vulnerability. Security of information on publicly accessible websites must be viewed in the context of an organization's overall OPSEC posture.

Any further questions regarding website content should be forwarded to (insert unit OPSEC Program Manager/Coordinator contact info.) or SIPRNET Webpage: (insert unit OPSEC Program Manager/Coordinator SIPRNET website, if applicable).

APPENDIX L

OPSEC Training

L.1 GENERAL

The effective implementation of OPSEC begins with appropriate training. OPNAVINST 3432.1A, Operations Security, requires that “the appointed OPSEC program manager will complete core competency OPSEC training,” (Navy OPSEC Program Manager Course (J-2G-0966)). OPSEC training is essential because at the carrier strike group or expeditionary strike group levels and at many shore stations, the duties and responsibilities of the OPSEC program manager are a collateral function of the member’s primary duty. Failure to take advantage of formal OPSEC training places commands at a significant disadvantage in implementing OPSEC into their missions, functions, and tasks. It is strongly recommended that every command have, at a minimum, the OPSEC program manager receive formal training. Additionally, the Joint Forces Staff College and Joint OPSEC Support Element offer the Defense OPSEC Planner’s Course, which focuses on incorporating OPSEC into the planning process.

L.2 INTERAGENCY OPSEC SUPPORT STAFF

The IOSS is located at Fanx 3, Fort George G. Meade, MD, and is considered the national OPSEC authority. IOSS offers a variety of services to both the prospective and current OPSEC program manager, in the form of OPSEC-related materials and most importantly, training opportunities. Learn more about IOSS at https://www.iad.gov/ioss/. The user-friendly site offers OPSEC course schedules and descriptions, quota information and points of contact.

L.3 NAVY INFORMATION OPERATIONS COMMAND NORFOLK

NIOC-Norfolk, located at JEB Little Creek, Virginia Beach, VA, offers a variety of IO-related courses, including the Navy OPSEC Program Manager Course. This course is also offered at NIOC San Diego. It is required of program managers, and it highly recommended that all OPSEC practitioners attend. The course is available via Mobile Training Team, upon request.

L.3.1 OPSEC Program Manager Course

The Navy OPSEC Program Manager Course (CIN J-2G-0966) includes an introduction to OPSEC, discusses the intelligence threat and our vulnerabilities to that threat, describes the interrelationship of OPSEC with traditional security programs, details the application of OPSEC techniques to the planning process, and provides guidance in the development of command and unit OPSEC training and orientation programs. The course trains officers, enlisted, and civilian personnel assigned to operational billets on the commands and staffs of the Navy, other armed forces, and departments of defense organizations to coordinate preparations for OPSEC within the command or mission. The course provides students with the fundamental knowledge and skills to perform duties as an OPSEC program manager for a command or unit.

L.4 USMC OPSEC TRAINING

The Marine Corps’ OPSEC training requirements are outlined in Marine Corps Order 3070.2A. The following are the requirements, outlined in order:

1. Annual OPSEC training is required for total force to include contractors.

2. OPSEC Fundamentals (OPSE 1301) is required for OPSEC program managers.

3. OPSEC Analysis & Program Management (OPSE 2380 and OPSE 2390, or Service equivalent) is required for OPSEC program managers at the regimental or group level and higher.

4. OPSEC & Public Release Decisions (OPSE 1500) is required for OPSEC program managers, public affairs officers, family readiness officers, and Webmasters.

5. OPSEC & Internet Based Capabilities (OPSE 3500) is required for OPSEC program managers, public affairs officers, family readiness officers, and Webmasters.

The Marine OPSEC Support Team, as a part of the Marine Corps Information Operations Center in Quantico, VA, also provides OPSEC training and support to Marine Corps units.

APPENDIX M

Ombudsman and Family Readiness Officer Guidance

M.1 OVERVIEW

This appendix provides guidance for the command or command representative for discussing OPSEC with the Navy ombudsman or Marine Corps family readiness officer (FRO), and for family OPSEC awareness training during predeployment gatherings and family or spouse support meetings. Extracts from chapters 6 and 10, which covers OPSEC, the Internet, and social media, can help in discussions with the ombudsman or FRO and in OPSEC family awareness meetings.

M.2 WHAT IS OPSEC?

OPSEC keeps potential adversaries from discovering our critical information. As the name suggests, it protects operations—those planned, in progress, and already completed. Mission success depends on secrecy and surprise, which allows the Navy and Marine Corps to accomplish the mission quickly and with less risk.

M.3 WHO IS THE ADVERSARY?

Our adversaries are many and are often difficult to recognize. Obvious enemies who come to mind include members of terrorist organizations and people that unfriendly countries send to do harm to us and make U.S. military efforts fail. Others include individuals or governments that are collecting information that could be used against the U.S. in the future or that could potentially negatively impact mission, morale, and perhaps the U.S. economy. Finally, there are criminals looking for information for personal gain.

M.3.1 What Does the Adversary Seek?

Enemies of freedom want our information—all types—and they are not just pursuing the military member to get it. They are interested in you, the family member, for the information that you may not realize that you have.

The military has always closely guarded its classified information, but unclassified information could be just as damaging if an enemy with the intent to do harm gains the opportunity. Enemies can piece together small bits of ordinary unclassified information like puzzle pieces to gain a clearer picture of U.S. intentions and actions.

Below are excerpts from a handbook captured in 2002 from a building that housed members of the Al-Qaeda terrorist group that provide first-hand examples of what adversaries want:

"It is necessary to gather as much information about the location as possible. For instance:

1. Transportation

2. The area, appearance and setting

3. Traffic signals and pedestrian areas

4. Security personnel centers and government agencies

5. Embassies and consulates

6. Public parks

7. Amount and location of lighting.”

The description of the base or camp must contain the following:

1. Weapons

2. Location and size

3. Fortifications and guards

4. Numbers of soldiers and officers

5. Ammunition depot

6. Vehicles

7. Commander’s name, rank, arrivals and departures

8. Degree and speed of security

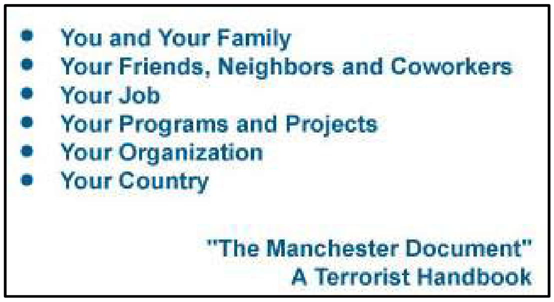
9. Sleeping and waking times

“Information about strategic buildings, establishments and military bases. Examples are ministries such as those of defense and internal security, airports, seaports, land border points, embassies and radio and TV stations.”

Seemingly harmless bits of information give adversaries a window into U.S. operations and opportunities to plot against the U.S. and its citizens. Some adversary targets are shown in figure M-1.

M.4 HOW DOES OPSEC APPLY AT HOME?

OPSEC blends seamlessly from military duty into personal lives. At home, health and safety of family members are as critical to unit morale and, ultimately, mission success as the bullets and bombs needed to destroy the enemy. OPSEC use at home protects loved ones and military mission as forces deploy worldwide, and also protects family members from becoming an indirect target of adversaries or criminals who would see your spouse’s absence as an opportunity or weakness for their own gain. Following are some examples of critical information that we urge you to review and protect before, during, and even after your loved one’s deployment.



- You and Your Family
- Your Friends, Neighbors and Coworkers
- Your Job
- Your Programs and Projects
- Your Organization
- Your Country

"The Manchester Document"
A Terrorist Handbook

Figure M-1. Adversary Targets

M.4.1 Critical Information You Should Protect

1. Dates, times, length of deployments, to include departure and arrival dates, using ship's name in correspondence and "Tiger Cruise" information

2. Places, names, ranks

3. Numbers of people, parts, or aircraft

4. En route stop locations

5. Hotels and room numbers

6. Personal information, addresses, and family names and addresses

7. Number and names of children

8. Social security numbers

9. Bank and credit card information.

M.4.2 Other Considerations

1. Military ID cards indicate you are military affiliated; use your driver's license instead when possible.

2. Military decals on your vehicle also indicate your military affiliation.

3. Do not send critical information to relatives or others via e-mail; it can be (and is) easily intercepted.

4. Teach OPSEC to your children; teach them what NOT to say when answering the telephone and give them safety tips to use when at home alone.

It is important to remember that OPSEC is a vital element in protecting mission and Service members and their loved ones. Each and every one of us plays a vital role in ensuring that 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 (see figure M-2).

OPSEC is a family affair. All family members and loved ones are part of the OPSEC team and need to protect the Navy's information to ensure our safety. Discuss OPSEC with all of your family!

Anything that effectively negates or reduces an adversary's ability to exploit our vulnerabilities.
Would you mail it to this man?
If the answer is "no,"
DON'T PUT IT ON THE WEB !

Figure M-2. Diligence in Operations Security

INTENTIONALLY BLANK

APPENDIX N

Sovereign Immunity

N.1 OVERVIEW

Appendix N provides policy that NAVADMIN 288/05 (CNO WASHINGTON DC 101814ZNOV05) establishes for commands regarding sovereign immunity of U.S. vessels in foreign ports.

N.2 SOVEREIGN IMMUNITY

As a matter of customary international law, all vessels owned or operated by a state and used for government noncommercial service are entitled to sovereign immunity. Vessels with this protection are immune from arrest or search (in foreign internal or territorial waters, or in international waters); immune from foreign taxation; exempt from any foreign state regulation requiring flying the flag of such foreign state (either in its ports or while passing through its territorial sea); and are entitled to exclusive control over persons aboard such vessels with respect to acts performed aboard. The privilege of sovereign immunity includes protecting the identity of personnel, stores, weapons, or other property aboard the vessel.

N.3 U.S. VESSELS' SOVEREIGN IMMUNITY

The United States asserts sovereign immunity for all U.S. vessels, as described above. Accordingly, providing a list of crew members (to include military and nonmilitary personnel) or any passengers aboard a U.S. vessel as a condition of entry into a port, or to satisfy local immigration officials upon arrival, is prohibited.

N.4 RESPONSE TO REQUESTS FOR CREW LISTS

Most host nations do not require that visiting U.S. vessels provide a crew list as a condition of port entry. For these nations, information about personnel aboard the vessel should not be volunteered. For host nations that request that a visiting U.S. vessel provide a list of personnel, naval component commanders shall adhere to the following:

1. Initially respond by informing the host nation that U.S. policy exempts foreign sovereign immune vessels visiting the United States from the requirement to provide crew lists in accordance with the same sovereign immunity principles that U.S. sovereign immune vessels claim.

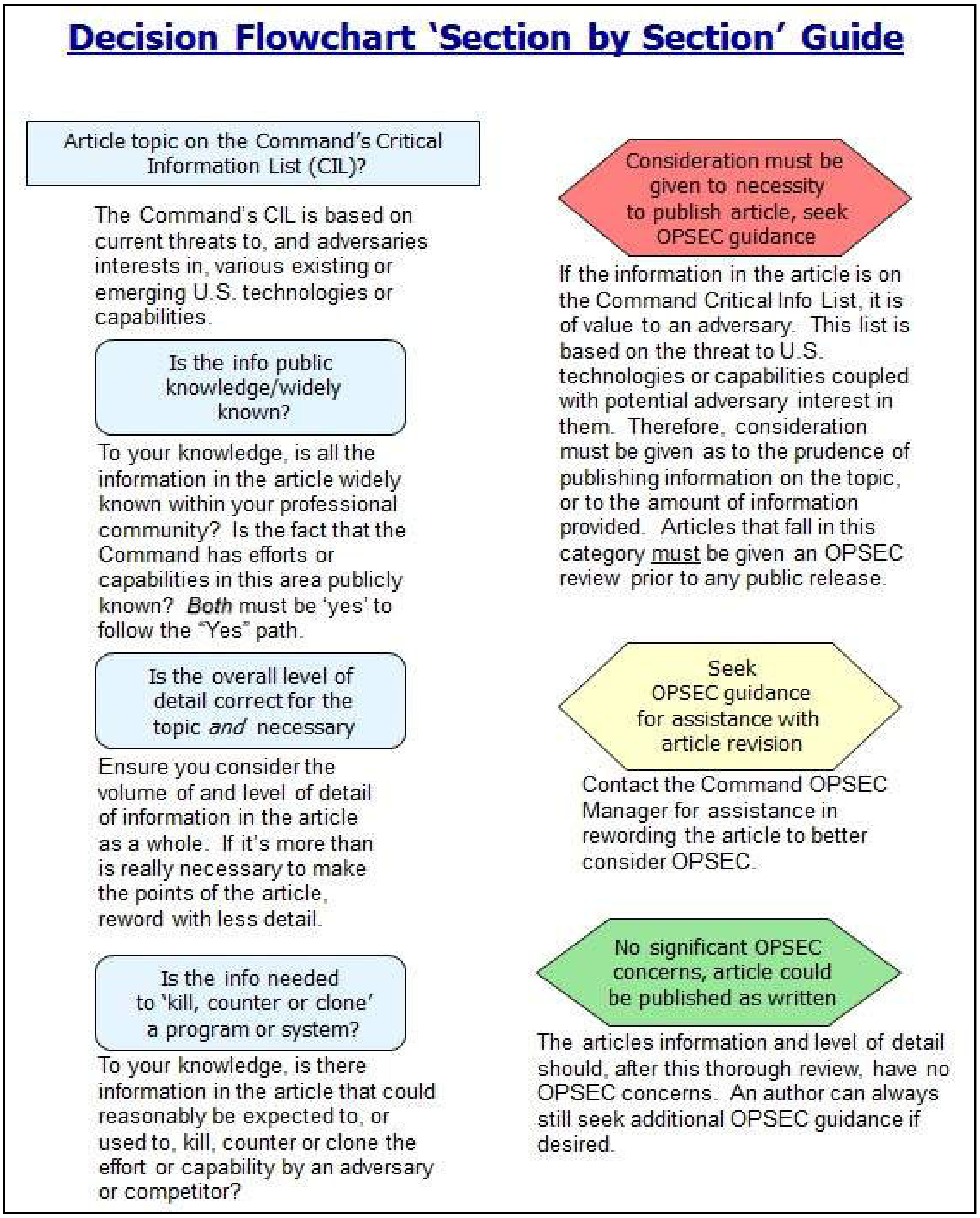
2. U.S. vessels shall not provide a crew list to host nation authorities under any circumstances; this includes military and nonmilitary personnel aboard the vessel.

3. If the host nation considers the alternatives to be unacceptable and continues pressing for more information, commanding officers shall consult with the responsible U.S. embassy country team and notify their chain of command up to the naval component commander.

INTENTIONALLY BLANK

APPENDIX O

Decision Flow Chart



Decision Flowchart 'Section by Section' Guide

Article topic on the Command's Critical Information List (CIL)?

The Command's CIL is based on current threats to, and adversaries interests in, various existing or emerging U.S. technologies or capabilities.

Is the info public knowledge/widely known?

To your knowledge, is all the information in the article widely known within your professional community? Is the fact that the Command has efforts or capabilities in this area publicly known? *Both* must be 'yes' to follow the "Yes" path.

Is the overall level of detail correct for the topic *and* necessary

Ensure you consider the volume of and level of detail of information in the article as a whole. If it's more than is really necessary to make the points of the article, reword with less detail.

Is the info needed to 'kill, counter or clone' a program or system?

To your knowledge, is there information in the article that could reasonably be expected to, or used to, kill, counter or clone the effort or capability by an adversary or competitor?

Consideration must be given to necessity to publish article, seek OPSEC guidance

If the information in the article is on the Command Critical Info List, it is of value to an adversary. This list is based on the threat to U.S. technologies or capabilities coupled with potential adversary interest in them. Therefore, consideration must be given as to the prudence of publishing information on the topic, or to the amount of information provided. Articles that fall in this category must be given an OPSEC review prior to any public release.

Seek OPSEC guidance for assistance with article revision

Contact the Command OPSEC Manager for assistance in rewording the article to better consider OPSEC.

No significant OPSEC concerns, article could be published as written

The articles information and level of detail should, after this thorough review, have no OPSEC concerns. An author can always still seek additional OPSEC guidance if desired.

Figure O-1. Decision Flowchart Section By Section Guide

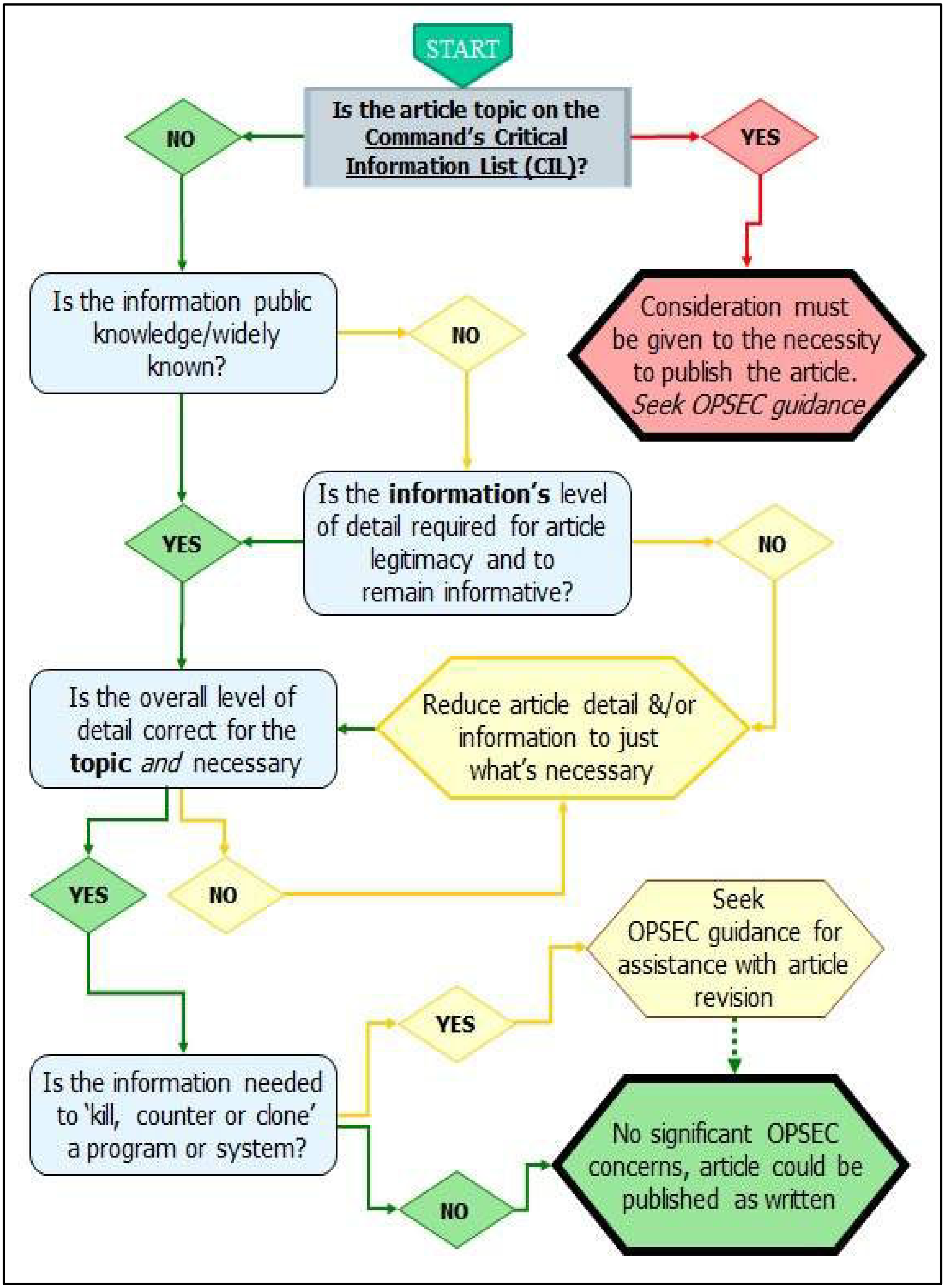

START
Is the article topic on the Command's Critical Information List (CIL)?
NO
YES
Consideration must be given to the necessity to publish the article. Seek OPSEC guidance
Is the information public knowledge/widely known?
NO
Is the information's level of detail required for article legitimacy and to remain informative?
YES
NO
Is the overall level of detail correct for the topic and necessary
Reduce article detail &/or information to just what's necessary
YES
NO
Seek OPSEC guidance for assistance with article revision
YES
Is the information needed to 'kill, counter or clone' a program or system?
NO
No significant OPSEC concerns, article could be published as written

Figure O-2. OPSEC Decision Flow Chart

APPENDIX P

Benchmarks

P.1 OPSEC-01—PROGRAM IMPLEMENTATION

References: CJCSI 3213.01D, DODD 5205.02E, MCTP 3-32B, MCO 3070.2A

Program implementation ensures that the command's OPSEC program is integrated throughout all levels of command. Program implementation also includes completing the administrative functions for OPSEC program development. See MCO 3070.2A, paragraphs 4b(15)(a), (16)(a), (17)(a) and 4b(17)(b)(2)(a).

1. Has the organization appointed in writing an OPSEC program manager or coordinator at the appropriate levels? (MCO 3070.2A, page 10, paragraph 4.b.(17)(b) (2))

2. Has the OPSEC program manager or coordinator completed the required training? (MCO 3070.2A, page 12, paragraphs 4.c.(3)(d) and (e))

3. Do the OPSEC program manager or coordinator have the proper security clearance (i.e., SECRET minimum)? (CJCSI 3213.01D, enclosure A, page A-10, paragraph 7.a)

4. Has the organization published an OPSEC policy, SOP, or annex document? (CJCSI 3213.01D, enclosure A, page A-5, paragraph 6.a.; and MCO 3070.2A, page 10, paragraph 4.b.(17)(c)(1))

5. Is OPSEC integrated into the installation's or organization's planning and operations? (CJCSI 3213-01D, enclosure A, page A-6, paragraph 6.g; and MCO 3070.2A, page 1, paragraph 1.b)

6. Is there an OPSEC tab for each operations order that the organization has produced? (CJCSI 3213.01D, enclosure A, page A-2, paragraph 1.f.(2), and page A-11, paragraph 7.b.(17))

7. Does the OPSEC program manager or coordinator ensure OPSEC assessments and surveys are conducted? (MCTP 3-32B, chapter 4, page 4-1, paragraph 4-1; and MCO 3070.2A, enclosure 6, page 6-2, paragraph 1.e.)

8. Does the command maintain a continuity binder and ensure that OPSEC policies, programs and plans are executed and evaluated through regular assessments? (CJCSI 3213.01D, enclosure A, page A-10, paragraph 7.b.(8))

9. Does the organization have an OPSEC support capability that provides for program development, training, assessments, surveys, and readiness training? (DODD-02E, enclosure 2, page 7, paragraph 11.h, and page 8, paragraph 13.c)

P.2 OPSEC-02—ANALYSIS (CRITICAL INFORMATION AND INDICATORS)

References: CJCSI 3213.01D, DODD 5205.02E, DODM 5205.02M, MCTP 3-32B, MCO 3070.2A

P.2.1 Critical Information List

A critical information list (CIL) is in place for all appropriate channels within the installation, and provides procedures to report disclosures of critical information so that mitigating actions can be implemented. Guidance is established for identifying and updating critical information as missions change. (DODD 5205.02E, enclosure 2, page 6, paragraph 11; MCO 3070.2A, paragraphs 4b(17)(c)(3) and 4c(3)(g); and The Social Corps: The USMC Social Media Principles Handbook, page 25)

1. Has the organization identified critical information and indicators, and established a regularly updated CIL? (DODM 5205.02M, appendix 1 to enclosure 3, page 13, paragraph 2.a. (5))

2. Has the commander approved that list been? (MCO 3070.2A, page 10, paragraph 4.b.(17)(c)(3))

3. Has the organization disseminated and published the list? (MCTP 3-32B, appendix C; and MCO 3070.2A, page 10, paragraph 4.b.(17)(c)(4))

P.2.2 Protection of Critical Information

Protection of critical information shall assess the quality and effectiveness of integrating OPSEC into the organization's policies and procedures. Protection of critical information is achieved through the proper handling, safeguarding, and destruction of critical information. (DODM 5205.02, enclosure 2 paragraph 6, and MCO 3070.2A, enclosure 1)

1. Do members of the organization utilize encryption techniques to protect critical information and all controlled unclassified information (CUI), such as FOUO data, when in-transit over unclassified networks? (DODM 5205.02M, enclosure 5, page 30, paragraph 1.b.(1), MCTP 3-32B, chapter 6, page 6-1, paragraph 6.2)

2. Are the identified OPSEC countermeasures effective in protecting the critical information by preventing the adversary from collecting and accurately interpreting the OPSEC indicators? (MCO 3070.2A, enclosure 6, page 6-6, paragraph 2.k.(6))

3. Does the command have a shred, personal electronic device (PED) and other supporting policies? (JP 3-13.3, chapter III, page III-8, paragraph 4.d. (10) and USMC Enterprise Cybersecurity Directive 005 Portable Electronic Devices (PED) version 2.0)

4. Is OPSEC integrated into the Command's policies on the personal use of email, the internet, and social media? Are the policies enforced? If so, has it been communicated effectively to all personnel in the command and who have access to the critical information? (CJCSI 3213.01D, enclosure A, page A-7, paragraph 6.h and enclosure A, page A-8, paragraph 6.j)

P.3 OPSEC-03—ANALYSIS (THREAT)

References: CJCSI 3213.01D, DODM 5205.02M, SECNAVI 3070.1, MCTP 3-32B, MCO 3070.2A

OPSEC threat analysis is necessary to develop appropriate measures. The threat analysis includes identifying potential adversaries and their associated capabilities and intentions to collect, analyze, and exploit critical information and indicators. (DODM 5205.02M, appendix 1 to enclosure 3, page 13, paragraph 2b; MCO 3070.2A, paragraph 4c(11) and enclosure 1; and The Social Corps: The USMC Social Media Principles Handbook, page 9)

1. Has an OPSEC threat analysis been performed? (MCO 3070.2A, enclosure 1, page 1-1, paragraph 3, and enclosure 6, page 6-4, paragraph 2.e)

2. Does the threat analysis identify likely foreign intelligence entity threat collectors? (CJCSI 3213.01D, enclosure B, page B-4, paragraph 7.e)

3. Does the OPSEC planner conduct threat analysis using intelligence assessments from related intelligence organizations (e.g., NCIS) to identify potential foreign intelligence entity collectors, both domestic and foreign, whenever necessitated by changes in tasking, environment, etc.? (MCTP 3-32B, chapter 3, page 3-3, paragraph 3-4)

4. Does the command receive threat information tailored to their specific needs? (SECNAV Instruction 3070.1, page 4, paragraph 4.o)

5. Does the threat analysis identify intent and capability for each threat? (MCTP 3-32B, chapter 6, page 6-1, paragraph 6.2)

P.4 OPSEC-04—ANALYSIS (VULNERABILITY)

References: DODM 5205.02M, MCO 3070.2A, MCTP 3-32B

The OPSEC vulnerability analysis is used to determine if an adversary is capable of collecting critical information or indicators, analyzing it, and then acting quickly enough to impact friendly objectives. Conducting exercises, red teaming, and analyzing operations help to identify vulnerabilities. (DODM 5205.02M, appendix 1 to enclosure 3, page 13, paragraph 2c; and MCO 3070.2A, enclosure 1)

1. Has a vulnerability analysis been performed? (MCO 3070.2A, enclosure 6, page 6-5, paragraph 6.i)

2. Have all vulnerabilities been addressed and protective measures identified to reduce risk to an acceptable level? (MCTP 3-32B, appendix G, page G-2, paragraph G.2)

P.5 OPSEC-05—ANALYSIS (RISK)

References: DODM 5205.02M, MCO 3070.2A, MCTP 3-32B

The OPSEC risk assessment is used to evaluate the risks to information based on susceptibility to intelligence collection and the anticipated severity of loss. It involves assessing the adversary's ability to exploit vulnerabilities that would lead to the exposure of critical information and the potential impact it would have on the mission. (DODM 5205.02M, appendix 1 to enclosure 3, page 13, paragraph 2d; and MCO 3070.2A, enclosure 1)

1. Has a risk assessment been performed for identified critical information? (MCO 3070.2A, enclosure 1, page 1-3, paragraph 5.d)

2. Does the commander know the impact to the mission? (MCTP 3-32B, appendix G, page G-2, paragraph G.2)

P.6 OPSEC-06—OPSEC MEASURES

References: JP 3-13.3, DODM 5205.02M, MCO 3070.2A

OPSEC measures and countermeasures are designed to prevent an adversary from detecting critical information, provide an alternative interpretation of critical information or indicators (deception), or deny the adversary's collection system. If the amount of risk is determined to be unacceptable, measures and countermeasures are then implemented to mitigate risk or to establish an acceptable level. (DODM 5205.02M, appendix 1 to enclosure 3, page 13, paragraph 2e; and MCO 3070.2A, enclosure 1)

1. Are OPSEC measures or countermeasures in place to protect sensitive and critical information? (MCO 3070.2A, page 10, paragraph 4.b.(17)(a))

2. How often are the measures reassessed? (MCO 3070.2A, enclosure 1, page 1-4, paragraph 6.c)

3. Have OPSEC measures or countermeasures been assessed to see if they are having the desired effect or are creating new indicators? (MCO 3070.2A, enclosure 1, page 1-4, paragraph 6.b)

4. Is there an established process in place to evaluate OPSEC measures and countermeasures? (MCO 3070.2A, enclosure 1, page 1-4, paragraph 6.c)

5. Have contractors been trained on local OPSEC requirements and the designated critical information and indicator list, along with the current OPSEC measures and countermeasures? (JP 3-13.3, page I-6, paragraph 7.f, and appendix A, page A-3, paragraphs 4.h and 4.k)

P.7 OPSEC-07—OPSEC WORKING GROUP

References: MCTP 3-32B, MCO 3070.2A

The OPSEC working group (OWG) ensures the command and family members maintain an acute OPSEC awareness. The responsibility of the group members is reporting their section respective application of the OPSEC process to their section heads. (MCO 3070.2A, paragraph 4c(a) and 4c(1)(a))

1. Has the organization formed an OPSEC working group? (MCO 3070.2A, page 4, paragraph 4.b.(1)(e))

2. Does the OPSEC working group include representatives from all major sections (tenant commands, if applicable) as well as public affairs, information security, and web administrators? (CJCSI 3213.01D, enclosure A, page A-11, paragraph 7.b. (13); MCTP 3-32B, appendix H, page H-1, paragraph H.1; and MCO 3070.2A, page 5, paragraph 4.b.(1)(h)(2); page 6, paragraphs 4.b.(2)(d), (3)(b), (4)(c), and (5)(b); page 7, paragraphs 4.b.(6)(b), (7)(b), and (8)(g); page 8, paragraphs 4.b.(9)(d), (10)(c), (11)(c), (12)(b), (13)(b), and (14)(b); and page 9, paragraphs 4.b.(15)(e) and (16)(f))

3. How often does the OWG meet and what are the actions that the OWG supports and performs? (MCTP 3-32B, appendix H, page H-1, paragraph H.2)

P.8 OPSEC-08—TRAINING AND AWARENESS

References: CJCSI 3213.01D, DODD 5205.02E, DODM 5205.02M, SECNAVI 3070.2, MCTP 3-32B, MCO 3070.2A

OPSEC training and awareness is essential because failure to take advantage of formal OPSEC training places commands at a significant disadvantage in implementing OPSEC in their missions, functions, and tasks. The risk of exposure to critical or classified information (alone or through compilation) is mitigated by providing OPSEC awareness training and guidance. (DODD 5205.02E, enclosure 2, page 7, paragraph 11.k; MCTP 3-32B, appendix L, page L-1, paragraph L.1; MCO 3070.2A, paragraphs 4b(1)(g)(3), 4c(1)(a), (c), (d), and (e), 4c(3)(e), 4c(3)(g), and 5b(2); and The Social Corps: The USMC Social Media Principles Handbook, page 25)

1. What type of initial OPSEC training does the workforce, to include contractors, receive upon joining the organization? (DODD 5205.02E, enclosure 2, page 8, paragraphs 12a through d, paragraphs 13.b and c, paragraph 15, and paragraph 16.a)

2. Does the command provide OPSEC orientation and awareness training to assigned personnel as well as ensuring OPSEC awareness training is conducted at least annually? (CJCSI 3213.01D, enclosure A, page A-7, paragraph 6.i.(1); CJCSI 3213.01D, enclosure B, page B-5, paragraph 10.a.(1); and DODM 5205.02M, enclosure 7, page 35, paragraph 3)

3. Does the organization’s workforce receive OPSEC training specific to the organization’s OPSEC program or policy? (CJCSI 3213.01D, enclosure B, page b-5, paragraph 10.a)

4. Is OPSEC training provided on threats, the critical information list, vulnerabilities, and measures and countermeasures? (DODM 5205.02-M, enclosure 3)

5. Are OPSEC program managers or coordinators, planners, IO professionals, and intelligence personnel supporting OPSEC planning receiving additional training for reviewing information for public release? (MCO 3070.2A, page 11, paragraph 4b(17)(c)(7))

6. Are PA personnel, family readiness officers, contracting personnel, Webmasters, and FOIA officers receiving additional OPSEC training specific to their duties according to Table 1 in MCO 3070.2A? (MCO 3070.2A, page 11, paragraph 4b(17)(c)(9))

7. How do DOD family members and others who require access to critical information receive OPSEC awareness instruction and support? (CJCSI 3213.01D, enclosure A, page A-8, paragraph i.4, and enclosure B, page b-6, paragraph 10.d)

8. Has the command developed area-specific OPSEC training for deploying Service members prior to their arrival in theater (combatant commands)? (MCTP 3-32B, chapter 6, page 6-1, paragraph 6.2.; chapter 10, page 10-1, paragraphs 10.1 and 10.2)

9. Does the command provide and document OPSEC training prior to granting individuals access to any DON NIPRNET, SIPRNET, or other information technology? (SECNAV Instruction 3070.1, page 3, paragraph 4.h)

P.9 OPSEC-09—OPSEC REVIEW

References: CJCSI 3213.01D, DODM 5205.02M, MCTP 3-32B, MCO 3070.2A

The command's responsibility extends beyond general public affairs considerations regarding the release of information but OPSEC and force protection. Formal OPSEC reviews are conducted to determine whether the command's sensitive and critical information is contained in information intended for public release, and to subsequently reduce any inadvertent disclosures. In addition, website reviews ensure all installations establishing publicly accessible websites conduct a review on the content to ensure that information posted on official sites does not compromise the unit's mission, national security, or place personnel at risk (DODM 5205.02M, enclosure 5; MCTP 3-32B, chapter 6, page 6-5, paragraph 6.5; MCO 3070.2A, paragraphs 4b(17)(c)(4) and paragraph 4c(1)(f); and The Social Corps: The USMC Social Media Principles Handbook, page 18)

1. Has an OPSEC review process been established to ensure command sensitive and critical information is not inadvertently disclosed to unauthorized entities? (DODM 5205.02M, enclosure 5, and CJCSI 3213.01D, enclosure A, page A-6, paragraph 6.b)

2. Are individuals responsible for releasing information to the public educated in OPSEC and release controls? (CJCSI 3213.01D, enclosure A, page A-7, paragraph 6.i(2))

3. Do any unclassified, publically available websites or Internet-based capabilities for which the public has access include any sensitive information that could put assets, missions or personnel at risk, or constitute—in aggregate—classified or sensitive information or contain information on critical information lists? (MCTP 3-32B, chapter 6, page 6-1)

4. Are unclassified, publically available websites and internet-based capabilities reviewed to ensure personnel lists, "roster boards," organizational charts, or command staff directories which show individuals' names, individuals' phone numbers, or email addresses that contain the individuals' names are not displayed? (MCO 3070.2A, page 3, paragraph 4.b.1.g.2, and MCO 3070.2A, page 14, paragraph 4.c.(4))

5. Does the OPSEC planner conduct public domain research on the unit for OPSEC indicators and vulnerabilities or disclosures, on sites to include social networking sites, bulletin boards, news releases, etc.? (MCTP 3-32B, chapter 6)

P.10 OPSEC-10—COORDINATION

References: DODM 5105.21M, DODD 5205.02E, DODM 5205.02M, DON FDO Manual, MCWP 3-33.3, MCTP 3-32B, MCO 3070.2A

In coordination with the PAO, the OPSEC program manager or coordinator must be an active participant in the process of deciding what information should be released to the public by balancing the legitimate information requirements of DOD and civilian audiences against the intelligence desires of the enemy. OPSEC is coordinated and integrated with other U.S. Government agencies, allies, and coalition partner programs, operations, and activities, as appropriate. (DODD 5205.02E, enclosure 2, page 7, paragraph 11i; MCTP 3-32B, chapter 9, page 9-1, paragraph 9.3; and MCO 3070.2A, paragraphs 4b(17)(c)(5) and 4c(1)(a)).

1. Do the OPSEC program manager or coordinator regularly liaise with Intelligence or Counterintelligence; Public Affairs; Security; FDO, FIOA or Contracting; and AT/FP representatives? (DODM 5205.02M, enclosure 2, page 7, paragraph 6.a.1; DODM 5205.02M, enclosure 5, page 30, paragraph 1.a.; and MCWP 3-33.3)

2. Is the OPSEC program manager or coordinator regularly involved in the operations and planning process for the command or organization? (DODD 5205.02E, enclosure 2, page 8, paragraphs 13.a. and 14; and DODM 5205.02M, enclosure 2, page 7, paragraphs 6.a.(1) and (13))

3. Is the OPSEC program manager or coordinator involved in the review process of information intended for public release? (MCTP 3-32B, appendix A, page A-6, figure A-2.10; and MCO 3070.2A, page 6, paragraph 4.b.(4) (a))

4. Is OPSEC integrated into AT/FP planning? (MCTP 3-32B, chapter 8)

5. Is written FDO guidance provided before information is released? (DON Foreign Disclosure Manual; and DODM 5105.21M, volume 2, enclosure 2, pages 26 through 27, paragraph 6.i.(2)(3))

P.11 OPSEC-11—CONTRACTING AND CONTRACTS

References: CJCSI 3213.01D, JP 3-13.3, DODD 5205.02E, DODM 5205.02M, MCTP 3-32B, MCO 3070.2A

In contracting and contracts, commanders and directors shall ensure that contractors supporting DOD activities use OPSEC to protect critical information for specified contracts and subcontracts. The requiring organization and Government Contracting Activity (GCA) shall impose OPSEC measures as contractual requirements when necessary. (DODM 5205.02M, enclosure 6, page 32, paragraph 1.a, and MCO 3070.2A, paragraphs 4b(17)(c)(8) and 4c(1)(f))

1. Has the command provided guidance for safeguarding critical information to contractors? (MCTP 3-32B, chapter 5, page 5-1, paragraphs 5.2 and 5.2.1; chapter 6, page 6-2, paragraph 6.3; and annex A, page A-6)

2. Are contract proposals that the organization produced reviewed for OPSEC concerns prior to publishing? (DODM 5205.02M, enclosure 6, page 32, paragraph 2)

3. Does the command ensure classified and unclassified contract requirements properly reflect OPSEC responsibilities and that these responsibilities are included in contracts when applicable? (DODM 5205.02M, enclosure 6, page 32, paragraph 2; and CJCSI 3213.01D, enclosure A, page A-6, paragraph 6.f)

4. Does the contract statement of work or DD Form 254 (Contract Security Specification) stipulate OPSEC training requirements? (JP 3-13.3, chapter 1, page 1-6, paragraph 7.f)

5. Are there provisions inserted into contracts and solicitations for contracting services that control the safeguarding, and subsequent release, of critical information? (MCO 3070.2A, page 11, 4b(17)(c)(6))

6. Does the OPSEC program manager or coordinator coordinate with contracting personnel to conduct a review for safeguarding critical information inserted into solicitations for contracting? (MCTP 3-32B, chapter 4, page 4-1, paragraph 4.2)

7. Does the contract officer technical representative or their designee monitor the training of contractors? (DODD 5205.02E, enclosure 2, page 5, paragraphs 4.a and b)

8. Has the contracting specialist received specialized OPSEC training? (MCTP 3-32B, appendix A, page A-2, paragraphs A.2.1.d and e)

P.12 OPSEC-12—SUBORDINATE UNITS

References: JP 3-13.3, MCTP 3-32B, MCO 3070.2A

OPSEC program managers or coordinators provide OPSEC planning guidance to their subordinate units to ensure that all units are operating under the same principles for a given area of responsibility (AOR). All units must adhere to higher command guidelines in order to maximize OPSEC effectiveness. (MCTP 3-32B, chapter 3, page 3-1, paragraph 3.1; and MCO 3070.2A, 4b(17)(c)(11))

1. Does the organization's OPSEC Program Manager assess the OPSEC programs of the organization's subordinate units? (JP 3-13.3, chapter IV, paragraph 2j(1); and MCTP 3-32B, chapter 3, page 3-1, paragraph 3.1)

2. Is OPSEC guidance and oversight provided to subordinate units? (MCTP 3-32B, chapter 3, page 3-1; and MCO 3070.2A, 4b(16)(d))

P.13 OPSEC-13—ANNUAL REPORT

References: MCTP 3-32B, MCO 3070.2A

If applicable, has the organization submitted input for the annual OPSEC report? (MCO 3070.2A, paragraphs 4b(15)(d) and 4c(8))

P.14 OPSEC-14—RESOURCES

References: DODD 5205.02E, DODM 5205.02M, MCTP 3-32B, MCO 3070.2A

Each installation shall maintain an OPSEC program that is resourced and focused on the protection of critical information. (DODM 5205.02M, enclosure 3, page 9, paragraph 1; and MCO 3070.2A, paragraphs 4c(3)(b) and paragraph 5b(2), and enclosure 6, paragraph 1.a)

Are dedicated manpower, funding, and resources available and prioritized to implement the OPSEC Program? (DODD 5205.02E, enclosure 2, page 7, paragraph 11d; and MCTP 3-32B, chapter 5, page 5-1, paragraph 5.2)

INTENTIONALLY BLANK

APPENDIX Q

OPSEC Indicators

Q.1 OPERATIONS SECURITY INDICATORS

OPSEC indicators are activities that can be heard, observed, or imaged. Indicators that an adversary or competitor obtains could result in adversary knowledge, or actions harmful to friendly intentions. They include such things as personnel or material actions and movements that can be observed; public releases, conversations or documents; and habitual procedures when conducting a given type of operation or test. All detectable indicators that convey or infer critical information must be identified and protected if determined vulnerable. OPSEC indicators are those friendly actions and open sources of information that adversary intelligence systems can potentially detect or obtain and then interpret in order to derive friendly critical information.

There are three main types of indicators:

1. Indicators establishing a profile. These give the observer or analyst patterns that show how activities are normally conducted within the activity.

2. Indicators showing deviations. These provide contrasts to the organization's normal activity. This helps the adversary gain an appreciation of intentions, preparations, and where and when the activity will occur.

3. Tip-off indicators. These provide the adversary with information on where to focus their attention and collection activities. These indicators are very significant when they warn an adversary of impending activity that may allow them to initiate a countermeasure.

The following are sample lists of indicators.

1. Operations indicators

   a. Stereotyped activities such as schedules, test preparations, range closures, etc.

   b. Visits of VIPs and other personnel associated with particular technology

   c. Abrupt changes or cancellations of schedules

   d. Purchasing specialized equipment

   e. Sending employees for increased project-related training

   f. Increased telephone calls, conferences, and longer working hours (including weekends)

   g. Coordination with subsidiaries that do not have proper safeguards for sensitive and classified information

   h. Holding rehearsals to test concepts of operations

   i. Senior officials and staff members making or attending unusual or increased number of trips and conferences.

2. Communications indicators

   a. Test reporting requirements that result in nonsecure transmission of POW information that should be passed over secure communications

   b. Talking around a classified subject

   c. Discussing personnel, intelligence, operations logistics and communications plans information over nonsecure communications

   d. Insisting that information be provided over nonsecure telephone or facsimile in order to inform or brief senior officials

   e. Arranging the itinerary of senior officials over nonsecure telephone

   f. Repetitive use of the same radio frequencies and call signs during operations or tests.

3. Administrative indicators

   a. Military orders

   b. Convening of planning and pre-execution conferences

   c. Distinctive emblems, logos, or markings on personnel, equipment, and supplies

   d. Transportation arrangements

   e. Medical care, preparation, and facilities

   f. Memoranda or advance plans

   g. Posting of schedules, orders, flight plans, manifests, duty rosters, etc.

   h. Leave cancellations and restrictions

   i. New facility activation

   j. Press releases, company brochures, or annual reports.

4. Logistics and maintenance support indicators.

   a. Volume and priority of requisitions

   b. Storing boxes or equipment labeled with the name of an operation or activity outside of a controlled area

   c. Prepositioning and establishment of logistics bases

   d. Procedural disparities in requisitioning and handling

   e. “Crash” maintenance programs

   f. Technical representatives

   g. Unusual equipment modifications

   h. Motor pool activity

i. Test equipment modifications

j. Test equipment turnover

k. Commercial services

l. Deviations or special logistics support procedures

m. Providing unique or highly visible physical security arrangements for reloading or guarding special equipment or facilities.

The following is a listing of indicators ordered in a different manner:

1. Common Indicators

   a. Access lists

   b. Conferences and meetings

   c. Ratings

   d. AIS needs

   e. Hours of operations

   f. Acronyms

   g. Code Words or nicknames

   h. Call signs

   i. Implementing procedures

   j. Evaluation results

   k. Planning conferences

   l. Requirement changes

   m. Security alerts

   n. Arrival times

   o. Departure times

   p. Milestone or suspense lists

   q. Formal agreements

   r. Locations of resources

   s. Mission statements

   t. Performance criteria

   u. Staff composition

v. Proficiency or quality ratings

w. Quality control procedures

x. Restrictions

y. Security procedures

z. Clearance requirements

aa. Access requirements

bb. Readiness state

cc. Emblems

dd. Activity intensity

ee. Planning conferences

ff. Equipment shortages

gg. Deficiencies

hh. Emergency procedures

ii. Security violations

jj. Security enhancements.

2. Planning Activity Indicators

a. Climatology

b. C2 procedures

c. Conferences

d. Exercises

e. Map coverage

f. Mission designators

g. Number of vehicles

h. Physical security procedures

i. Planned activity profile

j. Force structure

k. Intelligence activity

l. Scenarios

m. Security class guides

n. Tactical planning

o. Threat analysis.

3. Administration Activity Indicators

a. Accountability record

b. Administrative organization

c. Workload evaluation

d. Distribution records

e. Document receipts

f. Position descriptions

g. Incident reports

h. Correspondence records

i. Mail address changes

j. Mission statement

k. Inventory receipts

l. Publication records

m. Report distribution

n. Security clearances

o. Security investigations

p. Job requests.

4. Commercial Support Indicators

a. Facility use

b. Contract Security

c. Contract specifications

d. Memoranda of agreement (1\40A)

e. Technical reports

f. Trash disposal

g. Personnel movement

h. Staffing requirements

i. Courier service

j. Delivery and pickup times and places

k. Local government notifications

l. Local law enforcement

m. Requests for proposal (RFP)

n. Technical representative visits

o. Transportation support

p. Vehicle control

q. Vehicle rentals

r. Telephone service requests.

5. Staff Activity

a. Control procedures

b. Control responses

c. Leadership:

(1) Appearances in public

(2) Health

(3) Vacation schedule

(4) Personal affairs

(5) Tactical behavior.

d. Senior person identity

e. Staff composition

f. Liaison representative

g. Communications procedures

h. Organization structure

i. Staff experience level.

6. Communications Activity

a. Antenna type

b. Brevity code

c. Call signs

d. Communications discipline

e. Communications signatures

f. Encryption

g. Flow volume

h. Net/circuit designators

i. Net/circuit memberships

j. Operating instructions

k. Power requirements

l. Transmission times

m. Security procedures.

7. Financial Activities

a. Budget analysis

b. Budget justifications

c. Budget projections

d. Financial plans

e. Operating budgets

f. Advance payments

g. Travel requests

h. Travel vouchers.

8. Logistics Support

a. Cargo or shipment

b. Classification

c. Identification codes

d. Quantity

e. Origin

f. Priority

g. Size

h. Courier service

i. Movement assembly areas

j. Specialized vehicles

k. Traffic density

l. Schedules

m. Convoy assembly

n. Travel reservations

o. Commercial transport use.

9. Maintenance and Repair Activity

a. Vehicle identification

b. Nomenclature

c. Maintenance movements

d. Maintenance trends

e. Technical order changes

f. Test equipment

g. Repair schedule

h. Damage assessments

i. Failure rates

j. System-wide deficiencies.

10. Supply Activity

a. Stock numbers

b. Types of fuels and lubricants

c. Maps and charts

d. Inventory

e. Stockpile condition

f. Requisition priorities

g. Staging of material

h. Inventory timing

i. Storage capacity

j. Movements

k. Parts availability.

11. Personal Affairs

    a. Apparel

    b. Child care services

    c. Education program

    d. Immunizations records

    e. Newspaper delivery

    f. Passport

    g. Vehicle identification

    h. Security accesses

    i. Family routines

    j. Advance payments

    k. Housing

    l. Change of address

    m. Powers of attorney

    n. Will preparation

    o. Residence changes

    p. Hotel reservations

12. Personnel Activity

    a. Apparel

    b. Proficiency reports

    c. Staff strength

    d. Staff authorizations.

    e. Personnel locations

    f. Staff assignments

    g. Training activity

    h. Organization activations

    i. Skill shortages

    j. Special skill requirements

    k. Derogatory information.

13. Public Affairs Activity

    a. News articles

    b. News releases

    c. Advertisements

    d. Technical journal articles

    e. Requests for bid

    f. Economic impact statements

    g. Hazardous situations

    h. Hometown news releases

    i. Public appearances.

14. Schedules

    a. Delivery or pickup

    b. Dining hall

    c. VIP

    d. Intelligence briefing

    e. Operations briefing

    f. Laundry service

    g. Vacation

    h. Duty of the day

    i. Senior personnel itineraries

    j. Transportation.

15. Engineering and Services Support.

    a. Housing capacity

    b. Housing use

    c. Design factors

    d. Utility requirements

    e. Environmental impacts

    f. Firefighting capabilities

    g. Road usage

h. Trash disposal

i. New construction

j. Structure modifications

k. Facility maintenance

l. Facility usage.

INTENTIONALLY BLANK

REFERENCES

ALMAR 007/04

DOD 5205.2

DOD 5400.7R

DOD 8570.01-M

DODD 5205.02E

DODD 5240.01

DODD 8570.01

DODI 8550.01

DODM 5205.02-M

DON Social Media Handbook

JP 3-13.3

MARADMIN 071/04

Marine Corps Social Media Handbook

MCO 3070.2A

MCTP 3-32B

NAVADMIN 288/05

NSDD 298

NTISSD 600 (COMSEC Monitoring)

NTTP 3-13.2, Navy Information Operations Warfare Commander’s Manual

NTTP 3-13.3M

Operational Report-3 Navy Blue

Operational Report-3 Pinnacles

Operational Report-3 Unit Situation

OPNAVINST 2201.3

OPNAVINST 2201.3B

OPNAVINST 3430.26A

OPNAVINST 3431.1A

OPNAVINST 3432.1A

OPNAVINST 3432.1 series

OPNAVINST S5510.XX series

SECNAVINST 3070.2

SECNAVINST 5720.44C

TM 3-13.1-03, Computer Network Defense for the Carrier Strike Group/Expeditionary Strike Group

https://archive.org/web

https://www.digitalgov.gov/resources/negotiated-terms-of-service-agreements/

http://www.dimoc.mil/

http://dodcio.defense.gov/dodsection508/std_stmt.aspx

http://www.foia.n.mil

https://www.iad.gov/ioss/

http://iase.disa.mil/Pages/index.aspx

http://www.navy.mil/navydata/fact.asp

https://www.ncis.navy.smil.mil/

http://www.marines.com

http://www.marines.mil

http://www.marines.mil/Units/SiteRegistration.aspx

http://www.navy.com

https://www.portal.nwdc.navy.smil.mil/NDLS/pubs/forms/TACMEMOS.aspx

http://www.secnav.navy.mil/donhr/Site/Pages/No-Fear-Act.aspx

http://www.usa.gov/optout_instructions.shtml

http://www.usmc.mil

https://www.veteranscrisisline.net

GLOSSARY

acceptable level of risk. An authority's determination of the level of potential harm to an operation, program, or activity they are willing to accept for the unauthorized disclosure of critical or sensitive information.

adversary. A party acknowledged as potentially hostile to a friendly party and against which the use of force may be envisaged. (JP 1-02. Source: JP 3-0)

assessment. 1. A continuous process that measures the overall effectiveness of employing joint force capabilities during military operations. 2. Determination of the progress toward accomplishing a task, creating a condition, or achieving an objective. 3. Analysis of the security, effectiveness, and potential of an existing or planned intelligence activity. 4. Judgment of the motives, qualifications, and characteristics of present or prospective employees or "agents." (JP 1-02. Source: JP 3-0)

countermeasures. That form of military science that, by the employment of devices and/or techniques, has as its objective the impairment of operational effectiveness of enemy activity. (JP 1-02. Source: JP 3-13.1)

critical information. Specific facts about friendly intentions, capabilities, and activities needed by adversaries for them to plan and act effectively so as to guarantee failure or unacceptable consequences for friendly mission accomplishment. (JP 1-02. Source: JP 2-0)

critical information list. A list of critical information that has been fully coordinated and approved by the senior decision maker, and is used by all personnel in the organization to identify unclassified information requiring operations security measures.

data aggregation. Information collected from multiple sources and pieced together to form a bigger picture.

essential element of friendly information. Specific facts about friendly intentions, capabilities, and activities needed by adversaries to plan and execute effective operations against our forces.

impact. Cost in time, resources, personnel, or interference with other operations associated with implementing each possible operations security countermeasure versus the potential harmful effects on mission accomplishment resulting from an adversary's exploitation of a particular vulnerability.

indicator. 1. In intelligence usage, an item of information which reflects the intention or capability of an adversary to adopt or reject a course of action. (JP 1-02. Source: JP 2-0) 2. In operations security usage, data derived from friendly detectable actions and open-source information that an adversary can interpret and piece together to reach conclusions or estimates of friendly intentions, capabilities, or activities. (JP 1-02. Source: JP 3-13.3)

information environment. The aggregate of individuals, organizations, and systems that collect, process, disseminate, or act on information. (JP 1-02. Source: JP 3-13)

information operations. The integrated employment, during military operations, of information-related capabilities in concert with other lines of operation to influence, disrupt, corrupt, or usurp the decision-making of adversaries and potential adversaries while protecting our own. (JP 3-13)

information-related capability. A tool, technique, or activity employed within a dimension of the information environment that can be used to create effects and operationally desirable conditions.(JP 1-02. Source: JP 3-13)

measure of effectiveness. A criterion used to assess changes in system behavior, capability, or operational environment that is tied to measuring the attainment of an end state, achievement of an objective, or creation of an effect. (JP 1-02. Source: JP 3-0)

measure of effectiveness indicator. A unit, location, or event observed or measured, that can be used to assess a measure of effectiveness, often used to add quantitative data points to qualitative measures of effectiveness and can assist an information operations staff or cell in answering a question related to a qualitative measure of effectiveness.

measure of performance. A criterion used to assess friendly actions that is tied to measuring task accomplishment. (JP 1-02. Source: JP 3-0)

military deception. Actions executed to deliberately mislead adversary military, paramilitary, or violent extremist organization decision makers, thereby causing the adversary to take specific actions (or inactions) that will contribute to the accomplishment of the friendly mission. (JP 1-02. Source: JP 3-13.4)

military information support operations. Planned operations to convey selected information and indicators to foreign audiences to influence their emotions, motives, objective reasoning, and ultimately the behavior of foreign governments, organizations, groups, and individuals in a manner favorable to the originator's objectives. (JP 1-02. Source: JP 3-13.2)

open-source information. information that any member of the public could lawfully obtain by request or observation as well as other unclassified information that has limited public distribution or access. (JP 2-0)

open-source intelligence. Relevant information derived from the systematic collection, processing, and analysis of publicly available information in response to known or anticipated intelligence requirements. (JP 1-02. Source: JP 2-0)

operational environment. A composite of the conditions, circumstances, and influences that affect the employment of capabilities and bear on the decisions of the commander. (JP 1-02. Source: JP 3-0)

operations security. A capability that identifies and controls critical information, indicators of friendly force actions attendant to military operations, and incorporates countermeasures to reduce the risk of an adversary exploiting vulnerabilities. (JP 1-02. Source: JP 3-13.3)

operations security countermeasures. Methods and means to gain and maintain essential secrecy about critical information. (JP 3-13.3)

operations security indicator. Data derived from friendly detectable actions and open-source information that an adversary can interpret and piece together to reach conclusions or estimates of friendly intentions, capabilities, or activities. (JP 3-13.3)

operations security vulnerability. A condition in which friendly actions provide operations security indicators that may be obtained and accurately evaluated by an adversary in time to provide a basis for effective adversary decision making. (JP 3-13.3)

risk. Probability and severity of loss linked to hazards. (JP 1-02. Source: JP 5-0)

targeting. The process of selecting and prioritizing targets and matching the appropriate response to them, considering operational requirements and capabilities. (JP 1-02. Source: JP 3-0)

threat. 1. A generic term that refers to the armed forces, weapons, weapon systems, ammunition, and equipment of a potential adversary. 2. The intent of an agent to conduct operations that would disrupt the operation of a vessel, facility, or organization. The credibility of threat is based on the capability of the agent to carry out a disruptive act. (NTRP 1-02)

vulnerability. 1. The susceptibility of a nation or military force to any action by any means through which its war potential or combat effectiveness may be reduced or its will to fight diminished. (JP 3-01) 2. The characteristics of a system that cause it to suffer a definite degradation (incapability to perform the designated mission) as a result of having been subjected to a certain level of effects in an unnatural (man-made) hostile environment. (JP 3-60) 3. In information operations, a weakness in information system security design, procedures, implementation, or internal controls that could be exploited to gain unauthorized access to information or an information system. (JP 1-02. Source: JP 3-13)

INTENTIONALLY BLANK

LIST OF ACRONYMS AND ABBREVIATIONS

AIS	automated information system
ALMAR	All Marines
AO	area of operations
AT/FP	antiterrorism/force protection
CI	counterintelligence
CIL	critical information list
CO	commanding officer
COA	course of action
COMPUSEC	computer security
COMSEC	communications security
CONUS	continental United States
CPI	critical program information
CUI	controlled unclassified information
DAO	defense attaché office
DCO	defensive cyberspace operations
DIA	Defense Intelligence Agency
DISO	deception in support of operations security
DOD	Department of Defense
DODD	Department of Defense directive
DODM	Department of Defense message
DON	Department of the Navy
EEFI	essential element of friendly information
EPRM	Enterprise Protection Risk Management
FBI	Federal Bureau of Investigation

FLC	fleet logistics center
FOIA	Freedom of Information Act
FP	force protection
FRO	family readiness officer
GEOINT	geospatial intelligence
HN	host nation
HUMINT	human intelligence
IMINT	imagery intelligence
INFOSEC	information security
IO	information operations
IOSS	Interagency Operations Security Support Staff
IRC	information-related capability
IS	information system
ISIC	immediate superior in command
JCMA	joint communications security monitoring activity
KO	contracting officer
LAN	local area network
LE	law enforcement
LOGREQ	logistics requirement
MAA	master-at-arms
MARADMIN	Marine administrative message
MASINT	measurement and signature intelligence
MCO	Marine Corps order
MILDEC	military deception
MOST	Marine Operations Security Support Team
MTAC	Multiple Threat Alert Center
NETWARCOM	Navy Network Warfare Command
NCIS	Naval Criminal Investigative Service

NIOC	Navy information operations command
NIPRNET	Nonsecure Internet Protocol Router Network
NOST	Naval Operations Security Support Team
NSDD	national security decision directive
NTTP	Navy tactics, techniques, and procedures
OFRP	Optimized Fleet Response Plan
OPNAVINST	Chief of Naval Operations instruction
OPORD	operation order
OPSEC	operations security
OSCAR	operations security collaboration architecture
OSINT	open-source intelligence
PA	public affairs
PAO	public affairs officer
PII	personally identifiable information
PM	personnel misconduct
POD	plan of the day
SALUTE	size, activity, location, unit, time, and equipment
SAPCE	signature, associations, profiles, contrasts, and exposure
SECNAVINST	Secretary of the Navy instruction
SIGINT	signals intelligence
SIPRNET	SECRET Internet Protocol Router Network
SME	subject matter expert
SOP	standard operating procedure
SOPA	senior officer present afloat
STAAT	security training assistance and assessment team
TA	threat assessment
TV	television
U.S.	United States

USG	United States Government
USPACOM	United States Pacific Command
VIRIN	visual information record identification number
WRA	Web risk assessment
XO	executive officer
WMCT	Web measurement and customization technologies

LIST OF EFFECTIVE PAGES

Effective Pages	Page Numbers
SEP 2017	1 thru 18
SEP 2017	1-1, 1-2
SEP 2017	2-1 thru 2-4
SEP 2017	3-1 thru 3-8
SEP 2017	4-1 thru 4-10
SEP 2017	5-1, 5-2
SEP 2017	6-1 thru 6-4
SEP 2017	7-1 thru 7-4
SEP 2017	8-1, 8-2
SEP 2017	9-1 thru 9-4
SEP 2017	10-1, 10-2
SEP 2017	11-1 thru 11-4
SEP 2017	A-1 thru A-8
SEP 2017	B-1, B-2
SEP 2017	C-1 thru C-10
SEP 2017	D-1 thru D-4
SEP 2017	E-1 thru E-4
SEP 2017	F-1 thru F-14
SEP 2017	G-1 thru G-16
SEP 2017	H-1, H-2
SEP 2017	I-1, I-2
SEP 2017	J-1 thru J-6
SEP 2017	K-1 thru K-14
SEP 2017	L-1, L-2
SEP 2017	M-1 thru M-4
SEP 2017	N-1, N-2
SEP 2017	O-1, O-2
SEP 2017	P-1 thru P-8
SEP 2017	Q-1 thru Q-12
SEP 2017	Reference-1, Reference-2
SEP 2017	Glossary-1 thru Glossary-4
SEP 2017	LOAA-1 thru LOAA-4
SEP 2017	LEP-1, LEP-2

INTENTIONALLY BLANK

NTTP 3-13.3M/MCTP 3-32B
SEP 2017