U.S. NAVY **NTTP 3-54M**

U.S. MARINE CORPS **MCWP 3-40.9**

OPERATIONS SECURITY (OPSEC)

EDITION MARCH 2009

APPROVED FOR PUBLIC RELEASE; DISTRIBUTION IS UNLIMITED

PRIMARY REVIEW AUTHORITY:
NAVY INFORMATION OPERATIONS COMMAND (NIOC) NORFOLK

URGENT CHANGE/ERRATUM RECORD		
NUMBER	DATE	ENTERED BY

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

INTENTIONALLY BLANK

DEPARTMENT OF THE NAVY
NAVY WARFARE DEVELOPMENT COMMAND
NORFOLK, VA 23511
MARINE CORPS COMBAT DEVELOPMENT COMMAND
QUANTICO, VA 22134-5001

May 2009

LETTER OF PROMULGATION

1. NTTP 3-54M/MCWP 3-40.9, OPERATIONS SECURITY is UNCLASSIFIED. Handle in accordance with the administrative procedures contained in NTTP 1-01.

2. NTTP 3-54M/MCWP 3-40.9 is effective upon receipt and supersedes NTTP 3-54.3, OPERATIONS SECURITY dated August 2005. Destroy superseded material without report.

3. NTTP 3-54M/MCWP 3-40.9 provides the commander with an operations security (OPSEC) overview, OPSEC evolution, and guidance for the most crucial aspect of OPSEC, that of identifying critical information (CI). It explains the OPSEC process, also known as the OPSEC five-step process. This publication addresses the areas of OPSEC and force protection, public affairs officer (PAO) interaction, the role of the Naval Criminal Investigative Service (NCIS) in coordination with OPSEC, the OPSEC/OMBUDSMAN/KEY VOLUNTEER relationship and the conduct of OPSEC assessments. This publication includes separate chapters on Web page registration, Web risk assessment, and Red team activity. Appendices provide guidance to implement effective plans/programs at the individual unit, strike group, and shore establishment levels.

4. NTTP 3-54M/MCWP 3-40.9 is approved for public release; distribution is unlimited.

BY DIRECTION OF THE COMMANDANT OF THE MARINE CORPS

GEORGE J. FLYNN
Lieutenant General, U.S. Marine Corps
Deputy Commandant for Combat Development and Integration

WENDI B. CARPENTER
Commander
Navy Warfare Development Command

INTENTIONALLY BLANK

March 2009

PUBLICATION NOTICE

ROUTING

1. NTTP 3-54M/MCWP 3-40.9, Operations Security, is available in the Naval Warfare Library. It is effective upon receipt.

2. Summary. NTTP 3-54M/MCWP 3-40.9 is designed to promote operational effectiveness by helping prevent the inadvertent compromise of sensitive but unclassified activities, capabilities, or intentions.

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 and U.S. Marine Corps.

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.

Page No.

LIST OF ILLUSTRATIONS

Page No.

APPENDIX G — RISK ANALYSIS AND COUNTERMEASURE CONSIDERATIONS

APPENDIX K — WEB SITE SELF-ASSESSMENT CHECKLIST

APPENDIX M — OMBUDSMAN/KEY VOLUNTEER NETWORK GUIDANCE

INTENTIONALLY BLANK

PREFACE

NTTP 3-54M/MCWP 3-40.9 promotes operational effectiveness by helping prevent the inadvertent compromise of sensitive or classified activities, capabilities or intentions. 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: N5
1530 GILBERT STREET, SUITE 2128
NORFOLK, VA 23511

fleetpubs@nwdc.navy.mil

ORDERING DATA

Order printed copies of a publication using the Print on Demand (POD) system. A command may requisition a publication using standard military standard requisitioning and issue procedure (MILSTRIP) procedures or the Naval Supply Systems Command website called the Naval Logistics Library (https://nll1.ahf.nmci.navy.mil). An approved requisition is forwarded to the specific DAPS site at which the publication's electronic file is officially stored. Currently, two 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 website at: http://ndls.nwdc.navy.smil.mil or https://ndls.nwdc.navy.mil.

URGENT CHANGE RECOMMENDATIONS

When items for changes are considered to be urgent, send this information by message to the NIOC Norfolk (PLA: NAVIOCOM NOROFLK VA), info NWDC. Clearly identify and justify both the proposed change and its urgency. Information addressees should comment as appropriate. See accompanying sample for urgent change recommendation format on page 17.

ROUTINE CHANGE RECOMMENDATIONS

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

COMMANDER
NAVY WARFARE DEVELOPMENT COMMAND
ATTN: N5
1530 GILBERT STREET, SUITE 2128
NORFOLK, VA 23511

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 NAVIOCOM NOROFLK VA)//IOD//
INFO COMNAVWARDEVCOM NEWPORT RI//N5//
COMFLTFORCOM NORFOLK VA//JJJ//
COMPACFLT PEARL HARBOR HI//JJJ//
CG MCCDC QUANTICO VA//MID//
(Additional Commands as Appropriate)//JJJ//
BT
CLASSIFICATION//N03510//
MSGID/GENADMIN//(Organization ID)//
SUBJ/URGENT CHANGE RECOMMENDATION FOR NTTP 3-54//
REF/A/DOC/NTTP 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

Message provided for subject matter; 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, Paragraph 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, Paragraph 2.2, Line 4)
Add sentence at end of paragraph "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 Paragraph 2.2.

c. DELETE: (Page 4-2, Paragraph 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
COMUSPACFLT
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. OPSEC is a formal program that identifies and protects sensitive but unclassified information that ensures mission success. This document provides relevant U.S. Navy tactics, techniques, and procedures (NTTP) from a myriad of reference material to assist the command OPSEC officer/planner at the Maritime Operations Center (MOC) at the operational and tactical levels of war, and ultimately the commander, in taking prudent OPSEC considerations into account during day-to-day activities and the mission planning process.

1.2 SCOPE

NTTP 3-54 supports the commander by providing the MOC staffs and associated naval commands with an OPSEC overview, OPSEC evolution, and guidance for the most crucial aspect of OPSEC, that of identifying critical information (CI). It explains the OPSEC process, also known as the OPSEC five-step process. NTTP 3-54 addresses the areas of OPSEC and force protection, public affairs officer (PAO) interaction, the role of the Naval Criminal Investigative Service (NCIS) in coordination with OPSEC, the OPSEC/OMBUDSMAN/KEY VOLUNTEER relationship and the conduct of OPSEC assessments. The publication includes separate chapters on Web page registration, Web risk assessment, and Red team activity. Appendices provide guidance to implement effective plans/programs at the individual unit, strike group, and shore establishment levels.

1.3 BACKGROUND

NTTP 3-54 is the Department of the Navy (DON) comprehensive OPSEC guide that provide commanders a method to incorporate the OPSEC process into daily activities, exercises, and mission planning. OPNAVINST 3430.26 of 18 January 1995, the implementing instruction for using Navy and Marine Corps resources in information operations (IO), command and control warfare (C2W); OPNAVINST 3432.1 of 29 August 1995, Marine Corps Order (MCO) 3070.2; MCO 5720.75; Marine Administration Order 071/04; and All Marine (ALMAR) Order 007/04 served as the foundation for this publication. NTTP 3-54 integrates research, coordination, and personal interviews with national OPSEC entities, Joint and other Service personnel and materials, and Echelons 1 through 4 command personnel. This publication incorporates information collected and lessons learned over many years of naval OPSEC, afloat and ashore, and addresses newly emerging areas such as Web risk vulnerability, Web risk assessment, and OPSEC training.

1.4 SUMMARY

The purpose of NTTP 3-54 is to assist Navy and Marine Corps commands afloat and ashore practice good 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's Web-based design 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

Operations security is a systematic, proven process that identifies, controls, and protects generally sensitive but unclassified information about a mission, operation, or activity. 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. Good OPSEC helps to blind our enemies, forcing them to make decisions with insufficient information.

OPSEC is a core capability of IO, a primary warfare area, used in conjunction with computer network operations (CNO), military deception (MILDEC), electronic warfare (EW), and psychological operations (PSYOP). The integrated employment of IO, in concert with specified supporting and related capabilities, can influence, disrupt, corrupt, or usurp adversarial human and automated decisionmaking while protecting our own.

OPSEC …

- ▲ is an analytic process
- ▲ focuses on adversary capability & intent
- ▲ emphasizes the value of unclassified information.

OPSEC is a prerequisite for successful CNO, since compromise of a computer network attack (CNA) plan can degrade friendly operations; adversary knowledge of computer network defense (CND) plans increases the chances of our own network compromise. CNA can support OPSEC through Red teaming efforts (discussed in Chapter 7); CND is a prime OPSEC countermeasure.

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

OPSEC and MILDEC are more powerful and productive when mutually supporting. Since compromise can doom a deception plan, OPSEC is essential to deception. MILDEC can support OPSEC by permitting false indicators, drawing the enemy's attention away from CI associated with actual plans.

OPSEC and EW are mutually supporting. OPSEC supports EW by identifying critical components of an EW plan or operation. EW can support OPSEC with emissions control (EMCON) and by evaluating the effectiveness of EMCON measures as part of a Red team effort.

OPSEC and PSYOP are mutually supporting. OPSEC supports PSYOP in the same manner it supports other military operations by ensuring that CI is protected. PSYOP supports OPSEC by ensuring that OPSEC indicators are not included in PSYOP public messages.

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, could reveal sensitive or CI. 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 to prevent aggregation with other information, revealing intentions, or capabilities. Aggregation of unclassified 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 a comprehensive OPSEC check sheet to assist commands in executing OPSEC programs.

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

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

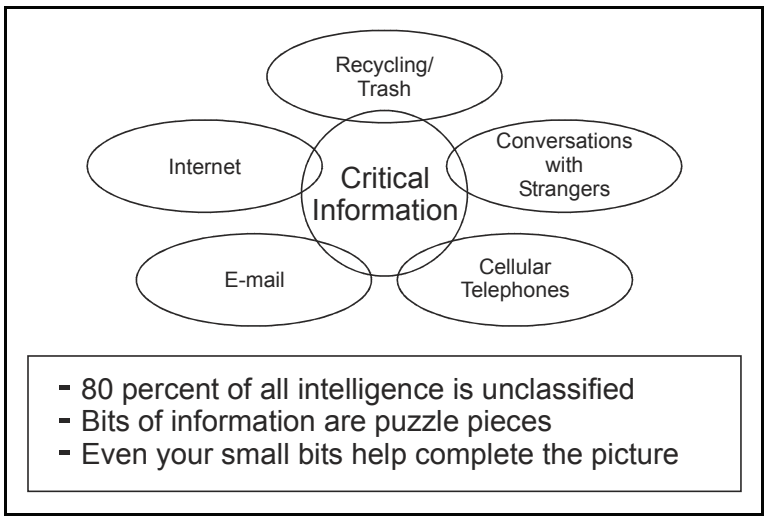

Figure 2-1. Data Aggregation

2.2 OPERATIONS SECURITY 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 IO core capabilities and other operational functions, such as maneuver. OPSEC is not security and is not intended to be a replacement for traditional security programs created to protect classified information. OPSEC is a process developed to deny adversaries publicly available indicators that are generally unclassified.

OPSEC is an operational function. Security, intelligence, and counterintelligence support its implementation. OPSEC officers and planners need expertise through formal training and comprehensive exposure in the mission

of the unit and application of the OPSEC process to choose the best course(s) of action to protect CI. OPSEC is an operations enabler, not a prohibitor.

In a naval context, OPSEC is a command responsibility that is trained for (see Appendix L), planned, and executed by the entire command. It requires, at a minimum, operationally mature OPSEC-trained officers/planners capable of coordinating functions for the commander and advising the commander on the best course(s) of action. OPSEC officers/planners ensure all participants (planners, operators, etc.) are aware of relevant CI and coordinate timely, resourced solutions. OPSEC officers 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. The OPSEC officer should be part of the "go/no-go" decision cycle. He communicates with the commander on process implementation and OPSEC best practices.

2.3 EVOLUTION OF OPERATIONS SECURITY

OPSEC, as a terminology, was coined in the late 1960s. It 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 modern times, 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 (attack at Normandy vice Pas de Calais) were effectively masked and false intentions were effectively portrayed. OPSEC and MILDEC were so effective that 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, since many enemy defensive forces were concentrated on Calais.

In Vietnam, 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 "Arc Light" missions over South Vietnam and of tactical fighter-bomber "Rolling Thunder" missions against North Vietnam. Counterintelligence and security personnel conducted investigations to find sources of leaks of classified information. 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 were able to destroy roughly 75 percent of our drone aircraft and rendered bombing missions ineffective by launching anti-aircraft defenses and implementing passive defenses on the ground (usually by vacating targeted areas).

The USPACOM OPSEC team identified that Notices to Airmen concerning drone, Arc Light and Rolling Thunder operations 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 disclosing altitudes, times, and locations for entry and exit of the flights into and out of the South Vietnam Air Defense Identification Zone, the enemy could make reasonably accurate predictions as to where and when the strikes would take place. By initiating permanent altitude reservations and entry/exit points, the need for forewarning was eliminated and the enemy's ability to deduce targets from entry and exit points was effectively neutralized.

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; others did not. When refueling operations were required, refueling for specific targets took place at specific points. They were easily detected by radar well in advance of the refueling mission, were easily identified by nonchanging clear-text call signs, and based on the time the refueling operations took place, the enemy could make reasonably accurate predictions as to where and when the strikes would take place.

Drone operations were frequently compromised by formatted messages sent 24 hours in advance concerning the flights of the C-130s that carried the drones. 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 on-line communications security (COMSEC) devices, drone loss rates dropped by 60 percent.

Following the success of these initial OPSEC studies by USPACOM in 1967, a team was established within USPACOM (J-3) that conducted approximately 55 additional OPSEC studies throughout the Pacific Theater. These studies continued to search out the vulnerabilities of CI to enemy threats and recommend viable countermeasures which, when instituted, enhanced operational effectiveness. The value of these studies was recognized by the Chairman of the Joint Chiefs of Staff (CJCS), (General Wheeler) who, in May 1968, proclaimed that, "…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. For example, OPERATION EAGLE CLAW, the attempt to rescue U.S. hostages in Iran in April 1980, 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 pre-attack 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 between 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, we 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 OPSEC failure. The openness and complacency of our society and many of our institutions permitted Al-Qaeda to thoroughly scrutinize our immigration practices, law enforcement procedures, intelligence capabilities and limitations, and our aviation system procedures. These conditions allowed the terrorists to enter the U.S., evade observation, obtain flight training, choose ideal aircraft (fully fueled/light passenger loads), circumvent airport/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 OPSEC syndicates or working groups for allied or coalition exercises and operations as early in planning as possible to establish OPSEC policy.

CHAPTER 3

Operations Security Process

3.1 SCOPE

The protection of essential elements of friendly information (EEFI) and subsequently, CI, is essential to the success of the OPSEC process. Failure to recognize EEFI/CI renders a commander ineffective against revealing operational/mission-related vulnerabilities, and thus conducting risk assessment and enacting countermeasures against a real or potential threat. The OPSEC process (see Figure 3-1), also known as the OPSEC five-step process, is the enabling vehicle for OPSEC planning. It provides the required information for the OPSEC portion of any plan or activity. Chapter 3 takes the OPSEC officer/planner through the five-step process, providing comprehensive guidance to produce an effective OPSEC plan. Immediate superior in command (ISIC) OPSEC officers 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. The five-step process is a proven method for safeguarding CI. OPSEC planning must closely coordinate with internal operations planning efforts and with the planning of supported or supporting units. Applying the process during the planning phase of any event or operation will greatly enhance the commander's effectiveness in identifying and protecting relevant CI. Sections 3.3 through 3.7 describe the five steps.

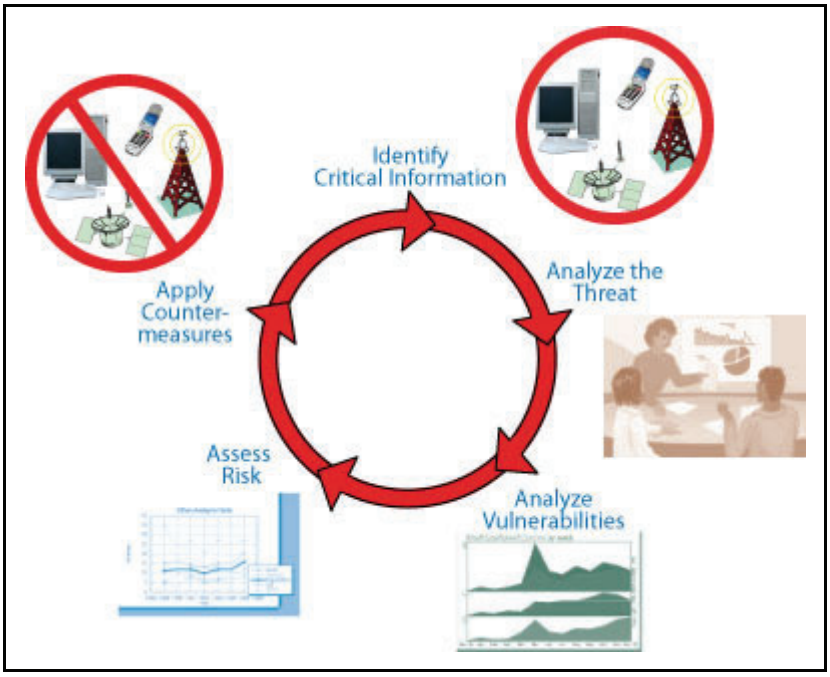

Figure 3-1. The Operations Security Process

3.2 ESSENTIAL ELEMENTS OF FRIENDLY INFORMATION

Planners need to establish EEFI—key information adversaries likely will 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 CI.

While assessing and comparing friendly-versus-adversary capabilities during the environment awareness and shaping process, as discussed in NTTP 3-13.2 (Information Operations Warfare Commander's Manual), for a specific operation or activity, the commanding officer and staff seek to identify the questions they think the adversary will ask about friendly intentions, capabilities, and activities.

Appendix B contains a generic list of questions, the answers to which may help the OPSEC officer/planner establish EEFI.

The successful application of OPSEC methodology depends upon the detailed/accurate identification of mission-related CI. Since CI is unique to the mission, compiling a single list of CI for the Navy and Marine Corps is impractical. However, it is feasible to create a generic list of CI, giving commanders and/or OPSEC planners the flexibility to expand generic categories of CI 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, and/or coalition) activities, intentions, capabilities, or limitations an adversary seeks in order to gain a military, political, diplomatic, economic, or technological advantage. Such information, if revealed to an adversary prematurely, may prevent or complicate mission accomplishment, reduce mission effectiveness, damage friendly resources, or cause loss of life. CI usually involves a few key elements of information concerning friendly activities or intentions that may significantly degrade mission effectiveness if revealed to an adversary. 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 the OPSEC officer/planner identify CI; Appendix C provides a list of generic CI in the form of an "all hands" memorandum. Derived from EEFI, CI includes only that information vitally needed by an adversary. Identifying CI 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 adversary success.

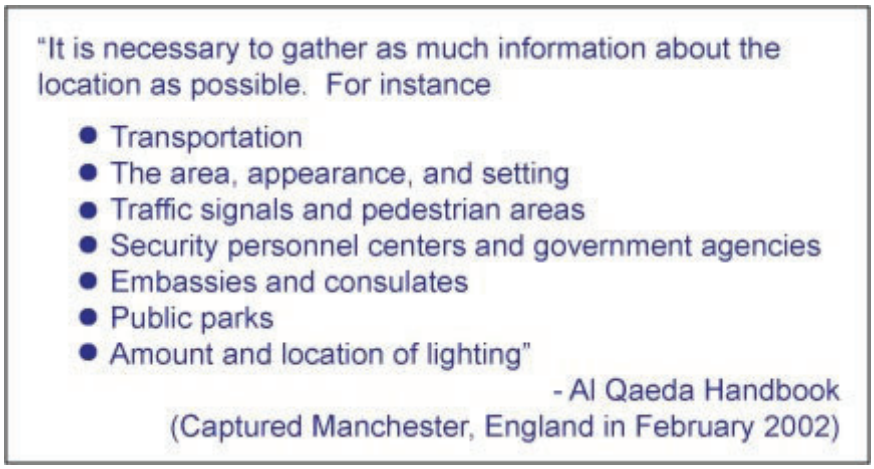

Figure 3-2. Example 1 of Critical Information

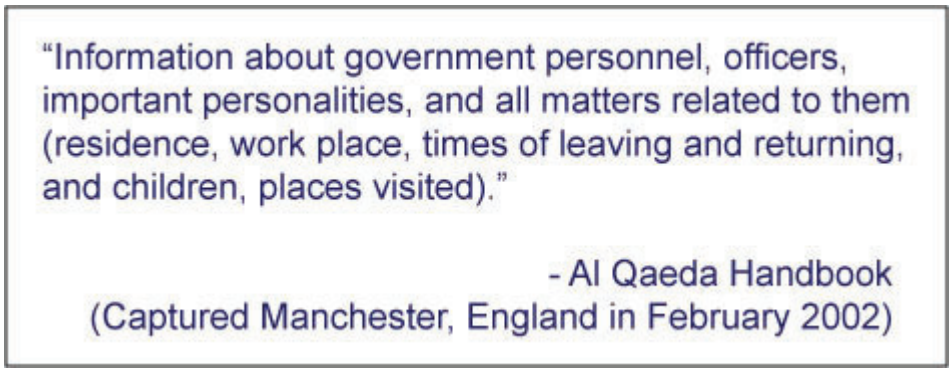

Figure 3-3. Example 2 of Critical Information

CI is listed in the OPSEC portion of an operation plan, operation order (OPORD), or command instruction. Examples of an OPORD and instructions are provided as Appendices D and E, respectively.

3.4 STEP TWO: THREAT ASSESSMENT

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 and their associated capabilities, limitations, and intentions to collect, analyze, and use knowledge of our CI against us. The threat refers to more than an enemy agent hiding behind a rock. The following examples represent threats:

1. An unauthorized person attempting to acquire CI.

2. A person supplying CI to an adversary.

3. A person inadvertently providing CI information to an adversary.

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 CI to an adversary will often help determine the lengths to which an adversary would go to acquire it. Various counterintelligence and intelligence organizations such as the Defense Intelligence Agency (DIA), NCIS, the Federal Bureau of Investigation, 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. (The role of NCIS and how it can assist in the OPSEC process is discussed in detail in Chapter 8). OPSEC officers, working with intelligence and counterintelligence staffs and assisted by OPSEC survey personnel, 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 CI does the adversary already have about the operations? (What information is it too late or too costly, in terms of money or resources, to protect?)

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

A TA matrix provided as Appendix F will further assist the OPSEC officer/planner complete this phase of the process.

3.5 STEP THREE: VULNERABILITY ANALYSIS

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

> A vulnerability (i.e., a detectable, exploitable event) may or may not carry a security classification at the time of its identification; but must be protected from disclosure by administrative or security controls.

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 in different, yet complimentary approaches. COMSEC plays a large role in OPSEC. Our worst enemy may be a careless word, and COMSEC efforts can focus on specific communications exploitation possibilities. (Procedures for requesting COMSEC monitoring are located in Chapter 4.) Computer security (COMPUSEC) also relates to OPSEC. Computers and computer systems are critical sources of sensitive information and require protection regardless of how their data is stored: floppy disks, CDs, hard drives, etc. As a result, command COMSEC and COMPUSEC planners require good input that identifies existing vulnerabilities.

Continuing to work with the intelligence and counterintelligence staffs, OPSEC personnel research the following questions:

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

2. What indicators can the adversary actually collect?

3. What 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 CI, while indicators require some analysis to derive CI. For example, when discussing important information over a nonsecure phone, vulnerabilities exist because the adversary may collect CI 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 security, physical or administrative, 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.

3.6 STEP FOUR: RISK ASSESSMENT

Risk assessment or measuring the level of risk, has two components. First, planners analyze the OPSEC vulnerabilities identified in the vulnerability analysis and identify possible OPSEC countermeasures for each. Secondly, planners select OPSEC countermeasures for execution based on a risk assessment for presentation to the commanding officer and staffs. OPSEC officers, working with other planners and with the assistance of intelligence and counterintelligence 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, the potential effects such exploitation will have on operations, and provide a cost-benefit analysis of possible methods to control the availability of CI 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 the OPSEC officer/planner assess risk to a mission or activity, Appendix H provides a risk analysis chart template, an example risk analysis, and analysis ratings criteria. Proper use of these tools will greatly enhance a command's OPSEC posture.

3.7 STEP FIVE: MEASURES/COUNTERMEASURES

Operations Security measures/countermeasures preserve military capabilities by preventing adversarial exploitation of CI. Countermeasures mitigate or remove vulnerabilities that point to or divulge CI. They control CI by managing the raw data, enhance friendly force capabilities by increasing the potential for surprise, and augment 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 CI or indicators. This includes the use of protective measures to create closed information systems, use cryptographic protection, and standardized security procedures. COMSEC and COMPUSEC 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, POTS, cell phones) for the purpose of OPSEC and force protection. Prior to commencing sensitive planning or operations that could be compromised by inadvertent communications/information release, a River City condition should be considered with the following guidance. River City is an OPSEC countermeasure. 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 placed into an appropriate user 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 access by foreign human intelligence agents.

2. Provide alternative deceptive interpretations of an indicator. Sometimes controlling actions that reveal CI 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 his ability to obtain CI. This category includes electronic attack against technical collection platforms and physical destruction of intelligence fusion and analysis centers.

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 cost in time, resources, personnel, or interference with normal operations. 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 CI. For example, camouflaging previously unprotected facilities could indicate preparations for military action.

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

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 counterintelligence organizations will ensure OPSEC requirements receive the appropriate priority.

CHAPTER 4

The Operations Security 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 and ad hoc 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 will immediately improve its effectiveness by implementing corrective measures to discovered vulnerabilities.

All naval commands should conduct an annual OPSEC assessment to identify potential vulnerabilities and give the commander a holistic security assessment of operations. 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 hostile intelligence or terrorist threat, identifies existing or potential problem areas, and recommends methods and procedures to improve the OPSEC mission posture.

There are two types of OPSEC assessments: command (internal), conducted annually; and formal (external), conducted every three years and also known as a survey. This chapter focuses on the internal assessment; however, it also includes procedures for requesting external assessments.

Operations Security assessments offer the opportunity 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 (i.e., a new AOR 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.

4.2 OPERATIONS SECURITY COLLABORATION ARCHITECTURE

The operations security collaboration architecture (OSCAR) risk analysis tool is an interactive, automated, risk assessment process that will assist planners and program managers in the evaluation of risks posed to an organization's CI.

The primary goal of OSCAR is to assist the OPSEC program manager in designating appropriate OPSEC measures to meet the commander's OPSEC risk level expectations. The OSCAR process organizes information and challenges the OPSEC program manager to identify information and processes which will produce the most accurate OPSEC analysis for the organization. OSCAR does not provide automated answers. Instead, it automates the thought process and leads the user to workable solutions to correct an organization's OPSEC issues.

OSCAR will give inexperienced OPSEC program managers a clear advantage through the captured experience of seasoned OPSEC professionals. OSCAR was developed in collaboration with OPSEC professionals from the Interagency OPSEC Support Staff, (IOSS) the Joint OPSEC Support Center, the Naval OPSEC Support Team,

(NOST) the Army's OPSEC Support Element at 1st IO Command, the Air Force Research Laboratory, and the Air Force, Army, and Navy OPSEC Program Managers.

The OPSEC risk analysis process is traditionally described as 1) identification of CI, 2) analysis of the threat, 3) assessment of vulnerabilities, 4) analysis of risk, and 5) development of countermeasures. OSCAR accomplishes these five steps in a manner that lends itself to automation. The OSCAR assessment begins by having the user identify the type of organization, its geographic location, and some basic operational information. The tool then presents the user with questions and data specific to that organization.

4.3 COMMAND OPERATIONS SECURITY ASSESSMENT

The OPSEC assessment, an evaluative process conducted annually, of an operation, activity, exercise, or support function determines the likelihood that commands can protect CI from the adversary's intelligence. The general methodology of an OPSEC assessment applies to all commands, but specific procedures vary depending on the mission(s) focus. An effective assessment requires cooperation and participation from all hands. Since members, 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 will improve mission effectiveness and performance through identification and elimination of potential vulnerabilities that may impact mission accomplishment.

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

A command assessment uses its own personnel to conduct an internal examination of the command's processes, 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. During a crisis(es), emphasis must be focused on identifying mission-related indicators that signal friendly intentions, capabilities, and/or limitations that will 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, will 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 OPSEC assessment. A successful assessment requires a team with expertise in the functional areas being examined, as well as team members who will bring an unbiased examination approach.

The OPSEC assessment identifies what an adversary might perceive and identify as potential information sources. The assessment represents a data gathering effort that differs from one done by a hostile country in that it uses minimal manpower, has a limited time frame, and does not resort to covert means. The 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.

Command 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/analysis, and reporting.

4.4 OPERATIONS SECURITY ASSESSMENT PLANNING

Conducting an effective 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 OPSEC assessment team meet in the planning phase.

4.4.1 Planning Actions

1. Preparations for an 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. Planners 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. Planners then determine which work unit(s), including associated support and management, uses the information with sensitivity in question. Additional work units can be added to the list during the assessment.

   c. The latitude of the assessment serves as a guide to select assessment members. As practicable, planners assign previous OPSEC assessment team members to maintain a high level of continuity.

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 I.

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

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

   c. 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.

   d. 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 no team members have previous assessment experience.

4. The team members' thorough 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 an initial, or verify current, CI list for the mission/project, and hold a dialogue on how to determine CI, 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/project personnel. Identification of CI is paramount to a successful assessment. Planners ensure that all parties—the assessed and the assessors—agree on the developed CI. Planners review and revalidate CI throughout the assessment, to include the briefing process, and after completion of the assessment to ensure that everyone agrees on what constitutes CI.

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

7. It is necessary to determine essential EEFI in order to develop a critical information list. (See Chapter 3.)

8. It is also necessary to determine sources of information—identify where an adversary may obtain CI.

> An extremely long CI list 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 CI.

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 will 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 to allow observation at those locations during the assessment phase.

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

    a. Purpose and scope

    b. Team members and their clearances

    c. Required briefings and orientations

    d. Time frame involved

    e. Administrative support requirements

    f. Signals security, COMSEC, COMPUSEC, and/or automated information system (AIS) monitoring requirements, if applicable.

11. The OPSEC team interviews command individuals to gain insight into daily processes and procedures. A standard set of questions will be developed by the OPSEC team 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 interviewing a representative sampling of each department/division.

4.4.2 Operations Security Assessment Analysis

During this phase, the OPSEC team correlates the data acquired by individual members. The team compares notes, assimilates data, and analyzes the operations, communications (if applicable), and intelligence aspects of the operation. Tentative conclusions may be validated or disproved through introduction of changes into suspected operational patterns. If evidence of foreign knowledge correlates to friendly action(s) 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.

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.

Correlation and analysis of data help the team refine the previously identified preliminary 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.

4.4.3 Operations Security Assessment Reporting

OPSEC assessment reports do not have a specific format. The report should provide a discussion of identified CI, indicators, and an adversary's intelligence capabilities, OPSEC vulnerabilities and recommended OPSEC measures to eliminate or reduce the vulnerabilities. Although some vulnerabilities may be virtually impossible to eliminate or reduce, planners should include them in the report to enable the commander to more realistically assess the operation or activity. The OPSEC officer tracks the findings until corrected. Many commands use a PowerPoint presentation for inbrief, outbrief, and plan of action and milestones. Assessment findings are kept within the command's chain of command. The command maintains results for three years.

Individuals may curtail or alter their normal practices/habits if informed of an assessment being conducted. Therefore, to obtain a clearer evaluation of the communications posture, it may be beneficial to refrain from announcing the assessment until after completion of initial monitoring.

4.5 EXTERNAL RESOURCES

Depending on the scope of the internal OPSEC assessment, commands may not possess the requisite expertise to either collect or analyze data. External resources (discussed in sections 4.4.1 through 4.4.3) can provide subject matter expertise.

4.5.1 Operations Security

Joint Publication 3-13.3, Operations Security requires external OPSEC assessments. Afloat and ashore commands submit requests for external OPSEC assessments to Commander, Naval Network Warfare Command via their immediate superior in command. The Interagency OPSEC Support Staff (IOSS), Joint IO Warfare Command's Joint OPSEC Support Center and the NIOC Norfolk Naval OPSEC Support Team (NOST) are chartered organizations to perform external assessments. The U.S. Marine Corps must submit requests for external assessment help via the chain of command to Headquarters, Marine Corps OPSEC Program Manager in the IO and Space Information Branch (which will prioritize and coordinate the assessment.)

4.5.2 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. A command desiring COMSEC support in conjunction with an OPSEC assessment 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 the site.

4.5.3 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 NCIS homepage: http://www.ncis.navy.smil.mil/.

4.5.4 Fleet Computer Network Defense

Fleet CND or Blue team personnel conduct a series of procedures to determine if vulnerabilities exist in a ship's AIS infrastructure. They also perform Red team functions designed to test the integrity of ships' networks. Detailed procedures on CND are located in NIOC TACMEMO 3-13.1-03, Computer Network Defense for the Carrier Strike Group/Expeditionary Strike Group. The publication can be accessed on line at: http://www.nioc-norfolk.navy.smil.mil/. Requests for these services are sent via unclassified message to NIOC Norfolk, Norfolk, VA (NAVIOCOM NORFOLK VA//N3//). The U. S. Marine Corps has its own CND Red team program imbedded in the Marine Corps Network Operations and Security Command and it may be reached via unclassified email at operationscenter@mcnosc.usmc.mil.

CHAPTER 5

Operations Security's Role in Operational Messages

5.1 SCOPE

Commands should give OPSEC key consideration when releasing operational messages or using email or chat in an official capacity. The judicious use of OPSEC reduces the risk of compromising sensitive unclassified information in a variety of messages and emails 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 logistic request (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 and Unit Situation Reports) 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, 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. Unclassified (UNCLAS) LOGREQs will not contain date and/or time of ship arrival. Specific date/time of ship arrival is considered sensitive and therefore, shall not be included in UNCLAS LOGREQ messages. (Classification Policy for Ship and SSN Movements (CINCLANTFLT 311538Z DEC 01) is provided as Appendix J.) The diplomatic clearance request specifies port visit dates and the FP LOGREQ supplement shall be used to specify date and time of ship's arrival. Both the diplomatic clearance request and FP LOGREQ supplement messages are normally classified at least Confidential — Releasable to the Host Nation, and provide adequate mechanisms for conveying sensitive ship's schedule information to required contractors and organizations. Defense Attaché Offices (DAO) and embassies are authorized to provide husbanding contractors the name of the ship, date, and time of arrival from the diplomatic clearance or FP LOGREQ supplement. However, it should be stressed to each contractor/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.

2. 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."

3. UNCLAS LOGREQ and FP LOGREQ supplemental messages will be transmitted immediately after release of the diplomatic clearance request message to facilitate adequate logistic support. Ships will

submit the UNCLAS LOGREQ to husbanding contractors over UNCLAS e-mail, but with no dates or times. This is particularly critical in ports without a nearby U.S. Navy support activity where substantial coordination is required.

4. When passing ship's arrival information over nonsecure circuits, including UNCLAS e-mail, use the following procedure. Refer to the LOGREQ by message date/time group; refer to data fields by line number. When discussing a specific ship's LOGREQ, individuals will not associate the ship's name, side number, or any other distinguishing characteristics with the information in the LOGREQ.

It is imperative that contractors understand the privileged nature of ship movement information, and that they are strongly discouraged from simultaneously discussing ship's name, time and date, or arrival when using the phone, e-mail or in conversation. Although information may be deemed unclassified by the Navy Security Manual or other guidance, dissemination of ship's port visit information should be controlled to the maximum extent possible. The husbanding contractor will require 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 DAO/American Embassy to obtain approval. This is due to potentially restrictive time lines regarding advance notification of port arrival.

5.3 CONCLUSION

The above listed measures are not all inclusive. Ultimately, common sense should prevail when drafting messages or sending email 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 World Wide Web (WWW) and the need for prudent OPSEC measures. Application of the OPSEC five-step process is imperative when placing information on the Web. Web site self-assessments are a useful tool in determining whether potential CI is on a command's Web site. Appendix L provides a self-assessment checklist. On-line 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 publicly accessible Web site information. Anything posted to the WWW is available to any adversary.

The worldwide connection of computer local area networks (LAN) and wide area networks such as the Non-Secure Internet Protocol Router Network (NIPRNET) make access to Department of Defense (DOD) information from anywhere in the world relatively easy. Separation between the NIPRNET and the WWW 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 (COMPUSEC and COMSEC) 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 and classified 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 current OPSEC methodology:

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

2. Determine the CI for the activity's operations and plans.

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

4. Determine the vulnerabilities—how protected are the Web pages? Remember, the hacker is generally the INFOSEC threat; the search engine and browser are generally the OPSEC threat.

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

6. Apply protection—combine INFOSEC, COMPUSEC, OPSEC, etc., tools to minimize information loss and vulnerability.

When applying the OPSEC process to information posted to Web sites, the activity will need to 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 Web and, using various search engines, browsers, and certain aggregation methods, 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, such as unit history, emblems, command affiliation, etc., will have less time criticality than will 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 will become public knowledge over time, decreasing the sensitivity of the data. Subsequently, the same information will again become sensitive as redeployment dates and unit withdrawal specifics are planned. This will require 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: http://www.waybackmachine.com.

6.3 OPERATIONS SECURITY AND THE INTERNET

Operations Security officers should review their command's Web site through the eyes of the adversary, looking for CI that could reveal sensitive operations, movement of certain assets, personal information about U.S. citizens and employees, and technological data. Possible sources of vulnerable data are shown in Figure 6-1.

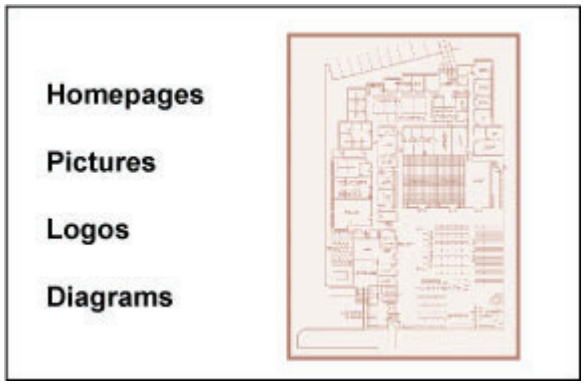

Figure 6-1. Possible Web Page Sources

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 will not include classified material, information that is sensitive in nature, or information that could enable the recipient to infer classified information.

Only information of value to the general public and that does not require additional protection should be posted to publicly accessible sites on the WWW. Information requiring additional protection, such as FOR OFFICIAL USE ONLY (FOUO) or SENSITIVE BUT UNCLASSIFIED information, 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 be placed on Web sites with security and access controls.

It is not necessary for our adversaries (see Figure 6-2) 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 Web site or those Web sites owned and operated by the command, privately by employees, or by DOD contractors. While the WWW 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 employees. The particular problem posed by today's technology is that Internet connectivity provides a singular user with new and increasingly efficient tools for reviewing and compiling information.

Figure 6-2. Adversaries on the Web

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, to select and develop knowledge about a target.

For OPSEC officers, 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 WWW 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; 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 officer/planner 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 officers/planners should caution employees on what should or should not be posted on DON publicly accessible Web sites and their own personal 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 to minimize inadvertent disclosure of CI.

6.3.1 Zero-based Web Site Security

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 CI 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 may not have been seen by a human observer, a satellite, a radio intercept operator, or the news. But with the proliferation of information technologies over the last three decades, 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 officers and planners must consider—the Internet. A disciplined approach to INFOSEC procedures, in conjunction with the OPSEC process, will ensure that sensitive but unclassified information is properly protected.

6.3.2 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 the 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 and putting their photo in a newsletter or on the Internet, may be putting them and their families at risk. Doing this may introduce command members to adversaries who probably otherwise never would have known about the individual.

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

6.4 ON-LINE SURVEYS AND WEB SITE ASSESSMENTS

The Navy Cyber Defense Operations Command (NCDOC) Norfolk, VA assists in identifying common network vulnerabilities on command systems. Upon command request, NCDOC will conduct an on-line survey (OLS) of systems attached to NIPRNET, SECRET Internet Protocol Router Network (SIPRNET), or Joint Worldwide Intelligence Communications System networks to assist Navy and Marine Corps commands in identifying

vulnerabilities on these systems. Commands may request an OLS through: https://www.ncdoc.navy.mil or https://www.ncdoc.navy.smil.mil.

NIOC Norfolk conducts Web risk assessments on all DON Web sites to identify and report OPSEC vulnerabilities. Services can be requested through http://www.nioc-norfolk.navy.smil.mil or www.nioc-norfolk.navy.mil.

6.5 REVIEW OF WEB SITES

Detailed Web site guidance and policy has been in existence since 1998, acknowledging the importance of the Web in communicating necessary information to the media and the American people. It requires commanders and personnel who authorize material to be posted on official Web sites to ensure that public Web sites contain information that should be accessible to the public while also ensuring that National and operational security are not compromised.

All activities that establish publicly accessible Web sites are responsible for ensuring that information posted on official sites does not compromise national security or place personnel at risk. The command's responsibility extends beyond general public affairs considerations regarding the release of information into the realm of OPSEC and force protection. Risk assessment and management procedures must be applied to ensure that the mission benefits gained by using the Web are carefully balanced against the potential risk to DOD interests, such as national security; the safety, security, and privacy of personnel or assets created by having aggregated information readily accessible to a worldwide audience.

Some information posted on government-owned, publicly accessible Web sites provides too much detail regarding DOD capabilities, infrastructure, personnel, and operational procedures. Such detail, when aggregated and correlated with information from other sources, can increase the vulnerability of DOD systems and jeopardize personnel and their families. Even if the command's Web site does not divulge too much information on the Internet, other organizations may publish the sensitive information provided to them—on-line compilations of conference slides are notorious examples. Automated Web-search tools make it easy to search all publicly accessible Web pages for information on a particular topic. If several sites leave pieces of sensitive data on the Internet, anyone who cares to look can compile a very clear picture of our operations and vulnerabilities. Therefore, a careful examination of the potential consequences of placing information on the Web must be conducted before making it available.

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 the NIOC Norfolk, Norfolk, VA. The Webmaster also has responsibility for reregistering the site annually, or when significant information changes, whichever occurs first. The registration form is available at: http://www.nioc-norfolk.navy.mil/wra/forms/websitereg.shtml.

INTENTIONALLY BLANK

CHAPTER 7

Red Team Vulnerability Assessments

7.1 BACKGROUND

In wargaming, the opposing force in a simulated military conflict is known as the "Red" team, and is used to reveal weaknesses in current military readiness. Red teaming operations improve organizational readiness and increase system administrators' security awareness of real-world IO vulnerabilities and incident recognition. The Red team tests procedures and methodologies by measuring/assessing organizational effectiveness in protection, detection, incident report/response, and reconstitution during a simulated IO attack.

7.2 RESPONSIBILITIES

All personnel tasked as Red team members should familiarize themselves with COMSEC monitoring procedures. Team members should review any additional directives (rules of engagement (ROE), concept of operations, standing ROE, Execution Order) from exercise coordinators and planners for prohibitive actions by the Red team.

The primary responsibility of the Red team officer is to assemble all exercise details and provide a daily status report to the requesting/controlling authority or the appointed officer conducting the exercise (OCE).

The Red team exercise will commence upon approval of the Red team officer or operations chief. All Red team activity immediately ceases in the event of real-world activity, operational commitment, or when directed by higher authority.

Red team exercises consist of three phases:

1. Phase I – Discovery and Mapping. Red team members conduct a thorough search for information about the target in open sources. They examine information regarding the location, official operations, personnel, mission capabilities, tactical and nontactical systems, phone numbers, and points of contact. This information will be utilized to identify possible weaknesses and plan the exploitative phase of operations.

2. Phase II – Identifying Vulnerabilities/Risk Mitigation. Applying assessment tools to identify computer system security vulnerabilities identifies vulnerabilities, which will be used in phase 3 of the exercise.

3. Phase III – Exploitation/Attack. The Red team officer or the operations watch chief will review logs and technical data to gather a list of potential targets and coordinate with operational commanders (trusted agents) before proceeding. Systems to be attacked must be evaluated to determine if the safety of the systems will be on a "taboo list" and will remain off limits to the Red team. At no time will the Red team place equipment or personnel safety in peril. **Safety is paramount.**

Once coordinated with operational commanders, the Red team will be granted permission to attack specific systems/networks using a specific technique as stated in the ROE.

Upon completion of the exercise, the Red team will draft a wrap-up message and after action report (AAR). Both should be addressed to the operational commander, or appointed OCE, and forwarded through the chain of command for release. The AAR will be used to build a lessons learned database for release as a NCDOC advisory on potential weaknesses in DON networks.

7.3 ASSISTANCE

Commands may request a Red team vulnerability assessment via the NIOC Norfolk Web site: http://www.nioc-norfolk.navy.smil.mil.

CHAPTER 8

Naval Criminal Investigative Service Contributions to the Operations Security Process

8.1 SCOPE

This chapter provides an overview of the NCIS role in antiterrorism/force protection (AT/FP) and how information they provide can assist the commander when implementing the OPSEC process and making decisions.

8.2 OVERVIEW

Naval Criminal Investigative Service provides AT/FP support and services to the U.S. Navy and Marine Corps from 140 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.

The NCIS AT/FP program 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/transient locations and transit chokepoints.

8.3 MULTIPLE THREAT ALERT CENTERS

The NCIS Multiple Threat Alert Center (MTAC) is a state-of-the-art analysis and production center for terrorist, criminal, counterintelligence, and security information. Using data obtained from NCIS special agents worldwide and other government agencies, the MTAC produces threat and trend analyses for afloat and ashore DON commands. 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 (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/terrorism threats that are tailored to alert potentially affected DON assets.

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

4. Suspicious Incident Summaries. Daily reports listing suspicious incident reports to DOD personnel and facilities inside and outside the continental United States (CONUS).

5. Security Bulletins. Unclassified weekly reports of suspicious incidents and law enforcement information.

6. Force Protection Summaries. Messages that provide DIA threat levels for countries worldwide.

7. Threat Assessments. Tailored tasks 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.

8.4 SUPPORT TO ASHORE INSTALLATIONS

Naval Criminal Investigative Service maintains offices at all major Navy and Marine Corps installations. Ashore commanders have direct access to NCIS AT/FP support and services through 13 field offices and 140 field elements worldwide. NCIS participates in the Joint Staff Integrated Vulnerability Assessment Program, the Chief of Naval Operations Installation Vulnerability Assessment (CNOIVA) Program and the Port Integrated Vulnerability Assessment Program.

8.5 SUPPORT TO AFLOAT COMMANDS

Through the NCIS Country Referent Program, agents conduct routine visits to expeditionary ports, airfields, and exercise areas to establish and maintain working relationships with U.S. and foreign law enforcement, military, and intelligence counterparts, so TAs can be prepared for transiting units. Collection efforts are 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.

CHAPTER 9

The Operations Security Officer/Public Affairs Officer Relationship

9.1 OVERVIEW

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

9.2 OPERATIONS SECURITY AND PUBLIC AFFAIRS: DIFFERENT ROLES

Public affairs and IO objectives differ. 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. IO serves, in part, to influence foreign adversary audiences using psychological operations capabilities. While audiences and intent differ, both PA and IO utilize the dissemination of information, themes, and messages that are adapted to the audience and operational level.

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

Public affairs and IO activities directly support military objectives, counter adversary propaganda, and help to deter enemy actions. Although both PA and IO use planning, message development, and media analysis as tools, their aims differ with respect to audience and intent, and must therefore remain absolutely separate. The PAO and OPSEC officer/planner must nevertheless be aware of each other's activities for maximum effect and to achieve success.

One reason why coordination and collaboration between IO and PA is essential is to ensure PA maintains its credibility. While organizations may be inclined to create physically integrated PA/IO offices, such organizational constructs have the potential to compromise the commander's credibility with the media and public. It is important that organizational relationships do not diminish the command's PA capability or effectiveness. PAOs should work directly for the commander, and supporting PA personnel should be organized under the PAO. Meanwhile, it is the commander's duty to ensure PA and IO efforts are coordinated.

9.3 CONCLUSION

To the maximum extent possible, the PAO and OPSEC officer should coordinate the release of data relative to the mission or to impending potentially sensitive activity. In close coordination with the PAO, OPSEC officers 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 CI list should be provided to the PAO. The commander has the ultimate responsibility for assessing the releasability of information from the perspective of both traditional security and OPSEC.

INTENTIONALLY BLANK

CHAPTER 10

Operations Security Guidance for the Navy Ombudsman and Marine Corps Key Volunteer Network

10.1 SCOPE

This chapter discusses OPSEC considerations for the Navy ombudsman and Marine Corps Key Volunteer Network (KVN). It provides an overview of sensitive, unclassified information on the Internet and how, through data aggregation, it can lead to disclosure of EEFI and potentially, CI. Portions of this chapter, in conjunction with Appendix M, provide guidance for ombudsman and KVN families OPSEC awareness training during predeployment gatherings, family/spouse support meetings, and ombudsman/KVN-sponsored Web pages.

10.2 OMBUDSMAN PROGRAM

The Navy Family Ombudsman and KVN programs provide an important communications link between Navy/KVN families and Navy/Marine Corps commands. The ombudsman/KVN is an official representative of, and is personally selected by, the commanding officer and serves as the liaison between command families and the command. Most command leaders agree that an effective ombudsman/KVN is a priceless asset, linking commands and families to ensure accurate and timely communication.

Navy and Marine Corps Family Service Centers provide formal ombudsman/KVN 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/KVN frequently can assist Service members who have problems.

Commanding officers correspond with their ombudsman/KVN 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/KVN 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. On line, it could be what one says over the course of weeks or months being pieced together.

10.3 WEB LOGGING

Despite stringent OPSEC measures, sensitive information regarding deployed units is readily available on the Internet. Web logging or "blogging," a type of on line journal used by some Navy/Marine Corps personnel and their family members to document a deployment, provides substantial unclassified information on deployed military personnel and units. Ombudsman/KVN or family support group newsletters published on the Internet, as well as unofficial Navy and Marine Corps-related Web sites, augment this information. 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.

Military related blogs, or "miliblogs," are permitted as long as they do not violate OPSEC. Most miliblogs, as a single source of information, do not violate OPSEC guidelines. Some Navy and Marine Corps commanders require review of miliblogs for possible security violations prior to posting. Despite this safeguard, hyperlinks provided within some miliblogs facilitate the collection of additional information that, when combined, reveal sensitive information. An example of this follows:

> A recently published article in the *Wall Street Journal* on miliblogs provided links to official and unofficial military Web sites. Using web links featured in this article, the Counterintelligence Field Activity (West) accessed a miliblog entitled, "Journal of a Military Wife." The miliblog provided information concerning the author's spouse, his unit, and hyperlinks to family support group newsletters. Although an alias was used in the miliblog, 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 miliblog. 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, to develop a comprehensive snapshot of the unit, its assigned personnel and their families.

10.4 INFORMATION OBTAINED

Unclassified open source data obtained from miliblogs, family support group newsletter sites, unofficial military Web sites and on line 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. Deployment location.
   h. Mission of the headquarters and subordinate units.
   i. Force protection mission of the unit at Camp Doha, Kuwait.
2. Military member-related information
   a. Photographs of soldiers with family members identified by name.
   b. Route of travel for unit soldier on leave (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 residence addresses.

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

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

10.5 MULTIPLE USES OF INFORMATION

Terrorist groups could potentially use information gained from the Internet to target family members of deployed military personnel. In Iraq and Afghanistan, terrorists have successfully kidnapped and assassinated numerous Westerners in an attempt to influence U.S. foreign policy. To escalate this threat, Al-Qaeda or associated groups could 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 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 could use personnel information found in miliblogs and on military Internet sites to target family members of deployed personnel for fraud, burglary, or other criminal activity. As an 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.

Military and personal information gathered from the Internet provides Foreign Intelligence Services (FIS) 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 FIS exploitation operations.

10.6 IS THERE REALLY A RISK?

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. 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, its 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.

In addition to the aforementioned information, Appendix N represents a basic OPSEC primer for the ombudsman/ KVN. It is designed for use in teaching family members their OPSEC responsibilities.

APPENDIX A

Operations Security Checksheet

A.1 U. S. NAVY AFLOAT/STAFF

1. Is a strike group/staff OPSEC officer assigned?

   a. Is the strike group/staff OPSEC officer appointed in writing?

   b. Has the strike group/staff OPSEC officer attended the OPSEC Planner Course?

   c. Has the strike group/staff OPSEC officer completed OPSEC 1301?

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

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

2. Ensure OPSEC officers are assigned/designated onboard strike group units.

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

   b. Has the ship's OPSEC officers attended the OPSEC Planner Course?

   c. Has the ship's OPSEC officers completed OPSEC 1301?

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

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

3. Meet with all strike group OPSEC officers a minimum of 180 days prior to deployment or as feasible to discuss operations/missions and task with developing each unit's Critical Information.

4. Meet with all strike group OPSEC officers a minimum of 90 days prior to deployment to identify strike group's and individual unit's Critical Information.

5. Is a Web risk assessment from NIOC Norfolk requested for each unit in the strike group?

6. Task each unit to conduct an OPSEC assessment a minimum of 60 days prior to deployment and report completion date to strike group/staff OPSEC officer.

7. Ensure each unit conducts a predeployment briefing for Ombudsman and/or family members a minimum of 30 days prior to deployment and report completion to the strike group/staff OPSEC officer.

8. Encourage/ensure (depending of assignment of units) each unit conducts an annual assessment and report completion date to their ISIC.

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

1. Is an OPSEC officer assigned in writing at the command?

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

   b. Does the appointee have a projected rotation date greater than six months or a relief identified under training?

   c. Are visual aids identifying the OPSEC officer and department representatives aware of their responsibilities?

   d. Does the OPSEC officer attend command security awareness and education meetings and address OPSEC issues?

   e. Has the command OPSEC officer attended or requested to attend the Navy OPSEC course or IOSS Program Managers' Course?

2. Has the OPSEC officer established a continuity folder? (see Figure A-1.)

   a. Are current editions of all instructions, pamphlets, and directives (DOD 5205.2, Joint Pub 3-13.3, OPNAVINST 3432.1, OPNAVINST 3430.26) being maintained in support of the OPSEC program?

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

I. Letter of Appointment (Signed by Commander or Commanding Officer).

II. Points of Contact (Include name, grade, organization, office symbol, phone numbers, and e-mail addresses. Also include functionality of contact, i.e., practitioner, program manager, survey coordination, training support …)
   a. Internal
   b. External.

III. Authorities and Guidance (List and place internal documents here, have a list of external documents and the location at which they can be found.)

IV. Organizational Critical Information Lists by section/office (These can be as detailed or generic as desired, i.e., ARG_CCIRs, SOCOM_CCIRs, CVBG_CCIRs.rft)

V. Working Group Minutes
   a. Member names with contact information
   b. Current meeting minutes
   c. Historical meeting minutes (Do not have to physically be in the folder, but list and annotate where they may be found.)
   d. Activity schedule (Based on information discussed in meetings, state who, how, and what, when and where. When complete, annotate completion date and annotate.

VI. Training (Document who, what, when, where and how. Keep records here or refer to where these can be found.)
   a. Annual unit/organizational calendar
   b. Schedule of training sessions (annotate completion dates when complete)
   c. List of people who you rely on to conduct the training and their contact information
   d. Compilation of training material and aids (ensure you state where each can be found).

VII. Assessments (Document who, what, when, where, and how. Keep records here or refer to where these can be found.)
   a. Schedule
   b. Schedule
   c. Schedule (etc.).

VIII. Marketing
   a. Methods
   b. Strategies
   c. Locations.

IX. "How to" instructions. (Must have IG standards and the heart of your program. Should include detailed descriptions on how to conduct each phase of your program. Think of this section as a very valuable self-teaching training tool for your replacement.)
   a. Assessment
   b. Marketing
   c. Training
   d. Working group.

X. Internal Assessment (3 years of data)
   a. Checklist
   b. Last inspection (include results/actions taken)
   c. Next scheduled.

XI. Miscellaneous information/file.

Figure A-1. Example of Continuity Folder

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 CI reviewed and approved by the commanding officer?

   c. Is the command CI displayed near unclassified communication systems?

4. Does the command OPSEC program promote 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 LAN, site TV, POD, etc.)

   c. Are OPSEC education materials reaching all command members?

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

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

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

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

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

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

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

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

6. Are the interrelationships of OPSEC, COMSEC, COMPUSEC, physical security, and information security programs clearly understood by the OPSEC officer?

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

8. Has the command OPSEC officer established and maintained liaison 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 arrival for duty?

10. Does command OPSEC training contain the following?

    a. The OPSEC methodology?

    b. Duty related mission CI and OPSEC indicators?

c. Foreign intelligence threat to the unit mission?

d. Individual responsibilities?

e. Operations Security and its relationship to the other core capabilities of IO?

11. Has the OPSEC officer reviewed command OPSEC plan/instruction annually, and if required, submitted an annual OPSEC status report to their respective staff?

12. Has an 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 CI changed significantly to warrant a new survey?

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 survey?

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 classified information? If so, are they protected? Who reviews them for OPSEC compliance?

16. Has a Web risk assessment been conducted on 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 officer on distribution for telecommunications monitoring (Joint Communications Security Monitor Activity) reports involving their command?

20. Does the OPSEC officer meet with the command ombudsman to provide training to the family? Has family training been incorporated with predeployment briefs?

A.3 OPERATIONS SECURITY PROGRAM REVIEW SAMPLE

Figure A-2 below is another OPSEC program checklist example.

ALL PURPOSE CHECKLIST		PAGE 1 OF 1 PAGES		
TITLE/SUBJECT/ACTIVITY/FUNCTIONAL AREA Operations Security (OPSEC) Program Review Checklist		OPR	DATE	
#	ITEM	YES	NO	N/A
1.	Has the organization appointed in writing an OPSEC program manager or coordinator at the appropriate level? (DoDD 5205.02, paragraph 5.3.1.1.; DoDM 5205.02, Encl. 3.)			
2.	Is the organization OPSEC manager or coordinator someone who is familiar with the operational aspects of the activity including the supporting intelligence, counterintelligence, and security countermeasures? (DoDD 5205.02, paragraph 2.2.)			
3.	Has the OPSEC manager or coordinator completed the appropriate training? (DoDM 5205.02, Encl. 7.)			
4.	Does the organization utilize the Naval OPSEC Support Team (NOST) capability that provides for program development, training, assessments, surveys, and readiness training? (DoDD 5205.02, paragraph 5.3.1.2.) [NOST website]			
5.	Has the OPSEC manager or coordinator developed local OPSEC guidance (regulations or operating procedures) for use of the OPSEC analytic process? (DoDD 5205.02, paragraph 5.3.1.3.)			
6.	Has the OPSEC manager or coordinator conducted an annual review and validation of the organization's OPSEC program? (DoDD 5205.02, paragraph 5.3.1.4.; DoDM 5205.02, Encl. 3.)			
7.	Does the OPSEC manager or coordinator submit an annual report? (DoDD 5205.02, paragraph 5.3.1.4.)			
8.	Does the OPSEC manager ensure OPSEC assessments and surveys are conducted? (DoDM 5205.02, Encl. 4.)			
9.	Does the OPSEC manager or coordinator provide sufficient support for subordinate units he or she has oversight for? (DoDD 5205.02, paragraph 5.3.1.5.)			
10.	Is the OPSEC manager or coordinator involved in the review process of information intended for public release? (DoDM 5205.02, Encl. 5.)			
11.	Has the organization ensured that CI is identified and updated as missions change? (DoD 5205.02, paragraph 5.3.4.)			
12.	Has the OPSEC manager or coordinator established, implemented, and maintained effective OPSEC education activities to include initial orientation and continuing and refresher training for assigned members? (DoDD 5205.02, paragraph 5.3.5.; DoDM 5205.02, Encl. 7.)			
13.	Does the OPSEC manager ensure OPSEC is included in force protection planning and local exercises when applicable? (DoDD 5205.02, paragraph 4.2.)			
14.	Does the OPSEC manager work with CIP planners to identify CI related to CIP? (DoDM 5205.02, Encl. 3.)			
15.	Are assigned personnel aware of the organization's CI? (DoDM 5205.02, Encl. 3.)			
16.	Has the OPSEC manager supplemented DoDD 5205.02 and DoDM 5205.02 and issued procedures for:			
	a. Integrating OPSEC planning into the planning, development, and implementation stages of net-centric programs and operating environments? (DoDM 5205.02, Encl. 2.)			
	b. Conducting OPSEC assessments and surveys? (DoDD 5205.02, paragraph 5.3.2.; DoDM 5205.02, Encl. 4.)			
	c. Handling, safeguarding, and destroying CI? (DoDM 5205.02, Encl. 5.)			
	d. A formal review of content for classification, sensitivity, sensitivity in the aggregate, determination of appropriate audience, and distribution and release controls when releasing information? (DoDD 5205.02, paragraph 5.3.3.; DoDM 5205.02, Encl. 5.)			
	e. Ensuring contract requirements properly reflect OPSEC requirements when appropriate? (DoD 5205.02, paragraph 5.3.6.; DoDM 5205.02, Encl. 6.)			

Figure A-2. OPSEC Program Review Checklist

A.4 U. S. MARINE CORPS INSPECTOR GENERAL CHECKLIST

The USMC portion of the Automated Inspection Reporting System Functional Area 481 OPSEC checklist can found at http://hqinet001.hqmc.usmc.mil/ig/Div_Inspections/AIRS%20Checklist/AIRS%20MONTHLY%20UPDATE/Checklist481.txt.

INTENTIONALLY BLANK

APPENDIX B

Essential Elements of Friendly Information Guideline

The following list is a general guideline to use in developing 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 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 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 EXAMPLES

Pages C-2, C-3, and 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 CI that, if compromised, could have adverse effects on the ship's personnel and thus, the overall mission. Every attempt should be made to ensure CI lists are unclassified to enable widest dissemination (facilitate 100 percent awareness). The example may be used by any activity, afloat or ashore, as it provides a comprehensive list of possible CI.

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 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 that CI can be harmful if released to our adversaries is key to good OPSEC. To this end, the development and frequent update of a CI 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 determined the following ship's information as CI:

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 two 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 date and transit the Turkish straits on date to participate in joint BSO with Ukrainian, Romanian, and Bulgarian forces.
b. The SEAL mission with the Greek Special Forces in support of the Olympics is classified SECRET.
c. We will evacuate the personnel and staff at U.S. Embassy in Liberia at 0500 on date.

COMMS

a. INMARSAT is down hard. Using HF communications ISO the mission.
b. Access to the JOTS system can be obtained by typing in cvn80 as the password.
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 in the storm — SATCOM is limited.
e. TACAN inoperative, flight operations suspended.

INTELLIGENCE

a. The ship's sole language linguist was medevac'd; we have no VHF voice intercept capability.
b. The map and location of area BRAVO provided by SEAL Team TWO is excellent.

LOGISTICS

a. Parts for both evaporators will take two weeks to arrive. Ship will be on water hours.
b. Ordered 2000 sets of desert cammies and boots. Scheduled to arrive on date and issued by date.

BUDGET

a. We've experienced a 40 percent decrease in spending as a result of cost-of-war cutbacks.

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. We're running out of ship drivers!

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 (SOP).
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, COMPUSEC, TEMPEST or physical security weaknesses).
b. Capabilities of communications equipment/system deficiencies—node(s), link(s), and impact.
c. Information revealing location of CI 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.2 CRITICAL INFORMATION TEMPLATE

Figure C-1 on the next page is a template available for use in determining CI.

Adversary:	
Adversary Objective:	
Adversary Strategy 1:	
What information would the adversary need to accomplish the strategy listed above?	
Adversary Strategy 2:	
What information would the adversary need to accomplish the strategy listed above?	
Adversary Strategy 3:	
What information would the adversary need to accomplish the strategy listed above?	
List any information that should be considered critical from a friendly point of view that is not already listed above.	

Figure C-1. Example of Critical Information Template

INTENTIONALLY BLANK

APPENDIX D

Sample Operations Security Plan

CLASSIFICATION: FOUO/CUI or higher

TITLE OF PROGRAM

OPERATIONS SECURITY PLAN

Date

Prepared by:

(signature)

Approved by:

(signature)

Typed Name

Typed Name

Title

Title

Prepared for:

Submitted by:

Organization

Name

Address

Address

The plan describes **(organization)** actions to implement a cost-effective OPSEC program for protecting **(organization, event, exercise, technology, etc.)**.

The OPSEC plan is an operations plan – not a security plan. Program personnel should consider it their plan to protect the U.S. technological lead and **(organization's)** competitive position. We anticipate the development or derivation of innovative concepts during the program. How well each team member protects sensitive information on this project may not only affect our national security, but may directly impact **(organization)**'s future business endeavors.

Requests for additional information or assistance should be submitted to **(POC name & phone number)**.

WARNING

This document contains technical data whose export is restricted by the Arms Export Control Act (Title 22, U.S.C., Sec 2751 et seq.) or Executive Order 12470. Violation of these export laws is subject to severe criminal penalties.

D.1 OPERATIONS SECURITY PLAN METHODOLOGY

Using the program specific CI, generate and complete a matrix table similar to Figure D-1 below. Each step of the OPSEC 5-step process will be evaluated and a matching value, high, medium high, medium, medium low and low will be entered into each corresponding block.

CRITICAL INFORMATION		COMMANDER HAS ESTABLISHED AN ACCEPTABLE RISK OF = High/Med/Low		THREAT	
1.				SIGINT	
2.				HUMINT	
3.				IMINT	
4.				OSINT	
5.				MASINT	
6.				CNO	
Vulnerability and/or Indicator	Probability	Impact	Risk	Countermeasure	Residual Risk

Figure D-1. Example Operations Security Plan Matrix Table – Blank Template

D.2 COMMANDER'S ACCEPTABLE RISK LEVEL

Based on the particular organizational and environmental factors, commanders will accept varying levels of risk. Inquire to the appropriate risk acceptance to support this OPSEC plan. For example, a headquarters facility in a suburban area may establish an acceptable risk level of low whereas a forward deployed mobile combat unit will establish an acceptable level of risk of medium high. If you are unable to obtain a risk decision, apply MEDIUM.

D.3 CRITICAL INFORMATION

CI is defined as elements or components of an research, development, and acquisition program that, if compromised, could cause significant degradation in mission effectiveness; shorten the expected combat-effective life of the system; reduce technological advantage; significantly alter program direction; or enable an adversary to defeat, counter, copy, or reverse engineer the technology or capability.

The value of CI can be based on its importance to both adversary and friendly objectives, and establishes subsequent impact to the organization or mission if that information is lost. Based on the scale in Figure D-2, assign a corresponding value from high to low for each CI identified.

	US	High	Medium High	Medium	Medium Low	Low
Adversary		Loss of Critical Information will have SEVERE impact on our ability to accomplish the mission	Loss of Critical Information will probably have SERIOUS impact on our ability to accomplish the mission	Loss of Critical Information will most likely have APPRECIABLE impact on our ability to accomplish the mission	Loss of Critical Information will possibly have MODERATE impact on our ability to accomplish the mission	Loss of Critical Information could have MINOR impact on our ability to accomplish the mission
High	Of CRITICAL Importance to an Adversary and Obtaining the Information Considerably Contributes to Meeting the Adversary's Objectives	High	Medium High	Medium High	Medium High	Medium High
Medium High	Of such CRUCIAL Importance to an adversary that Obtaining the Information Appreciably Contributes to Meeting the Adversary's Objectives	Medium High	Medium High	Medium High	Medium	Medium
Medium	Of such ESSENTIAL Importance to an Adversary that Obtaining the Information Greatly Contributes to Meeting the Adversary's Objectives	Medium High	Medium	Medium	Medium Low	Low
Medium Low	Of MODERATE Importance to an Adversary that Obtaining the Information Contributes to Meeting the Adversary's Objectives	Medium High	Medium Low	Medium Low	Low	Low
Low	Of MINOR Importance to an Adversary	Medium High	Low	Low	Low	Low

Figure D-2. Critical Information Matrix

D.4 THREATS — GENERAL APPLICABILITY

Based upon information provided by **(organization name)** and other government agencies, the threats applicable to the **(title)** efforts stem primarily from five sources:

1. signals intelligence (SIGINT)
2. HUMINT
3. OSINT
4. imagery intelligence (IMINT)
5. measurement and signature intelligence (MASINT)

Estimating the relevant threats posed by a specific adversary is based on the adversary's (or adversaries') known capabilities and intent to collect. Using the scale in Figure D-3, assign a value from high to low for the threat severity of known adversaries.

Intent		Capability: High	Capability: Medium High	Capability: Medium	Capability: Medium Low	Capability: Low
	Adversary	The Adversary's Collection Capability is HIGHLY developed and MOST LIKELY In place OR The Adversary receives equivalent data collection support from a HIGHLY capable 3rd party	The Adversary's Collection Capability is Significantly developed and PROBABLY In place OR The Adversary receives equivalent data collection support from a SIGNIFICANTLY capable 3rd party	The Adversary's Collection Capability is Possibly developed and LIKELY In place OR The Adversary receives equivalent data collection support from a CAPABLE 3rd party	The Adversary's Collection Capability is PROBABLY NOT developed and MOST LIKELY NOT In place OR The Adversary may receives equivalent data collection support from a 3rd party	The Adversary's Collection Capability is NOT developed OR does NOT receive data from a 3rd party
High	The Adversary is HIGHLY Motivated and a Successful Outcome SIGNIFICANTLY Contributes to Meeting the Adversary's Intended Objectives	High	Medium High	Medium High	Medium	Medium Low
Medium High	The Adversary is SIGNIFICANTLY Motivated and a Successful Outcome GREATLY Contributes to Meeting the Adversary's Intended Objectives	Medium High	Medium High	Medium High	Medium	Low
Medium	The Adversary is SUFFICIENTLY Motivated and a Successful Outcome WILL Contribute to Meeting the Adversary's Intended Objectives	Medium High	Medium	Medium	Medium Low	Low
Medium Low	The Adversary is MODERATELY Motivated and a Successful Outcome CAN Contribute to Meeting the Adversary's Intended Objectives	Medium	Medium Low	Medium Low	Medium Low	Low
Low	The Adversary is NOT Motivated to collect information	Medium Low	Low	Low	Low	Low

Figure D-3. Threat Matrix

D.5 VULNERABILITIES

Vulnerabilities of the program may reveal sensitive or classified information, operations, plans, and/or activities and are derived by comparing the threat to the sensitive aspects of the contract and assessing the OPSEC indicators. These vulnerabilities are specific to (**title**). Examples are:

1. Use of a commercial travel office, travel patterns, and travel practices.
2. Geographic separation of the program participants.
3. Limitations of export license(s).
4. Effectiveness of the product.

5. Sympathies of program personnel for adversary countries.

6. Outdoor testing with exposure to overhead (imagery) threats, HUMINT observation, etc.

7. Communications between test sites and program offices following testing.

8. Lack of procedures or failure to comply with those developed for controlling visits and documents/information release international partners and subcontractors.

9. Unauthorized access to specific unclassified performance parameters.

Calculating susceptibility of CI to adversary collection includes the identification of indicators that can also induce a susceptibility to adversary collection. Based on the scale in Figure D-4, assign a value from high to low for each vulnerability (and indicator) according to the likelihood it would offer an opportunity for exploitation.

HIGH	Exploitation of this vulnerability by an adversary will make CI susceptible to at least one intelligence collection discipline virtually any time the adversary chooses to collect.
MEDIUM HIGH	Exploitation of this vulnerability by an adversary will make CI susceptible to at least one intelligence collection discipline most of the time the adversary chooses to collect.
MEDIUM	The adversary's capability to exploit this vulnerability is not well developed but could frequently make CI susceptible to at least one intelligence collection discipline.
MEDIUM LOW	The adversary's capability to exploit this vulnerability is poorly developed, and CI is only occasionally susceptible to at least one intelligence collection discipline.
LOW	Potential for exploitation is negligible.

Figure D-4. Vulnerability Values

D.6 RISK ASSESSMENT

Risk is assessed as a measure of the probability that an adversary will be successful in collecting CI and the resultant cost to the mission (impact).

1. Probability is determined by multiplying a vulnerability value by the relative threat value. In other words, if the vulnerability involves susceptibility to HUMINT collection, the threat value would be specific to the adversary's HUMINT collection capability. In a situation where a single vulnerability might be exploited by multiple collection methodologies, use the highest rating for risk calculation.

2. Use Figure D-5 as a decision chart for probability, combining the values for threat and vulnerability.

Threat / Vulnerability	HI	MED HI	MED	MED LOW	LOW
HI	HI	MED HI	MED	MED LOW	LOW
MED HI	MED HI	MED	MED	MED LOW	LOW
MED	MED	MED	MED	LOW	LOW
MED LOW	MED LOW	MED LOW	LOW	LOW	LOW
LOW	LOW	LOW	LOW	LOW	LOW

Figure D-5. Probability of Critical Information Loss (Threat Severity X Vulnerability Level)

3. Determine the risk by multiplying probability times impact. The measure of impact in this example can be determined by reviewing the value of the CI that is susceptible to HUMINT collection. Should multiple items of CI be susceptible to exploitation by a given vulnerability, the analyst makes a decision on the combined value of that CI. Most often, the combined value is the highest value placed on any one CI item.

4. Use Figure D-6 as a decision chart for risk, combining the values for probability and impact. For example, if the threat is high and the vulnerability is medium high, the probability of compromise is medium high. If the value of the CI is medium high, the risk is medium.

Probability / Impact (CI Value)	HI	MED HI	MED	MED LOW	LOW
HI	HI	MED HI	MED	MED LOW	LOW
MED HI	MED HI	MED	MED	MED LOW	LOW
MED	MED	MED	MED	LOW	LOW
MED LOW	MED LOW	MED LOW	LOW	LOW	LOW
LOW	LOW	LOW	LOW	LOW	LOW

Figure D-6. Risk Assessment

D.7 OPERATIONS SECURITY MEASURES

Analysis of vulnerabilities identifies tentative OPSEC measures required to maintain essential secrecy. The most desirable OPSEC measure combines the highest protection with the least impact on (name) effectiveness. There are three categories of OPSEC measures.

1. Action Control – alternative ways of conducting actions and activities which avoid indicators that create vulnerabilities; actions taken within **(name)** to eliminate/prevent or control indicators; denies access to the sensitive information, operation, or activity by applying one or more of the traditional security measures (classification, physical security).

2. Countermeasures – Disruption of adversary information collection or gathering. Eliminate or modify the pattern or vulnerability.

3. Counter-analysis – Actions to cause misinterpretation of indicators by analysts. Apply deceptive measures.

An example of an OPSEC Plan that integrates all the processes together is provided in Figure D-7.

D.8 OPERATIONS SECURITY PLAN IMPLEMENTATION PRODUCT

Figure D-7 provides an example of integrating the complete OPSEC Plan process.

CRITICAL INFORMATION			ASSUME THE COMMANDER HAS ESTABLISHED AN ACCEPTABLE RISK OF = MEDIUM.		THREAT[1]	
1. Mission Times		Med High			SIGINT	High
2. Security Procedures		Med High			HUMINT	High
3. Specific Logistics Support		Med High			IMINT	Med High
4. Crew Names With Missions		High			OSINT	Med
5. Assets Assigned to Missions		High			MASINT	Med Lo
Vulnerability and/or Indicator		Probability[2]	Impact[3]	Risk	Countermeasure[4]	Residual Risk[5]
Use of open networks	High	High	High	High	Restrict coordination of mission activities to classified networks. Reduces the vulnerability to medium.	Medium
Use of commercial shipping	Med High	Med High	High	Med High	None immediately available.	Med High[6]
Crew member personal information on official Web pages	High	Med	High	Med	Bring unit Web pages into compliance with DOD policy. Conduct unit awareness. Reduces the vulnerability to medium.	Med
Stereotyped operations	Med	Med	High	Med	None required.	

[1] In this example, assume two adversaries with different intents and capabilities. The value entered here is the combined threat from both adversaries using the highest of the values. For instance, adversary 1 represents a medium SIGINT threat and adversary 2 represents a high SIGINT threat. High is used for the risk analysis. Adversary 1 represents a high HUMINT threat and adversary 2 represents a medium high HUMINT threat. High is used for the risk analysis.

[2] Use of open networks is susceptible to SIGINT; high threat times high vulnerability equals high probability. Use of commercial shipping makes CI susceptible to SIGINT, HUMINT, IMINT, and OSINT; the highest threat value is high, so high threat times medium high vulnerability equals medium high probability.

[3] Use of open networks could place all of the CI at risk. The combined impact of the adversary's exploitation of that CI would be high. Use of commercial shipping could potentially place CI items 3 and 5 at risk, with an impact value of high.

[4] If the commander's acceptable risk level is medium and the initial risk analysis is medium, no countermeasure is required. However, if a remedy is readily available and inexpensive, a countermeasure may still be recommended.

[5] By reducing the vulnerability to medium, the probability of exploitation is reduced to medium; medium times high impact equals medium risk.

[6] There may not always be an effective countermeasure available to reduce the vulnerability or otherwise mitigate the risk. By identifying this, the commander may determine whether that vulnerability is acceptable or may determine that more expensive countermeasures, or a change in the plan, might be warranted.

Figure D-7. Operations Security Plan Matrix Table – Completed Example

D.9 OPERATIONS SECURITY PLAN EXECUTION EVALUATION

After determining and selecting measures to protect CI, they should be evaluated to determine suitability for similar vulnerabilities.

Figure D-8 depicts a means of measuring measure effectiveness.

Vulnerability	Measure	Expected Outcome	Date Evaluated	Finding	% Measure Worked	Recommended Modifications
Use of open networks	Restrict coordination of mission activities to classified networks.	No evidence of mission coordination activities via open/publicly accessible networks/websites	31 Oct 08 1000 1500	No discussions overheard, no emails detected, no phone conversations detected; however, information was on website	80%	Continue to review Web site; remove or change data

Figure D-8. Evaluation Matrix

APPENDIX E

Sample Operations Security Instruction

Appendix E shows a sample OPSEC instruction.

DEPARTMENT OF THE NAVY
COMMAND LETTERHEAD

Reference Information
Date

COMMAND INSTRUCTION NUMBER XXXX.X

Subj: OPERATIONS SECURITY (OPSEC)

Ref:
(a) OPNAVINST 3432.1
(b) JCS Pub 3-54 of 24Jan97
(c) CJCSI 3213.01A
(d) DODDIR 5205.2
(e) NTTP 3-53.3

1. Purpose. To establish policy and provide guidance for implementing and managing (Command Name) Operations Security (OPSEC) Program.

2. Cancellation. (Prior instruction)

3. Background. Information operations (IO) are actions taken to affect adversary information and information systems while protecting one's own information and information systems. OPSEC supports, and is integrated with, the other elements of IO to deny an adversary the information needed for effective decision making and to focus and prioritize IO countermeasures to protect critical information (CI).

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 CI 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 Officer will conduct annual reviews 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. The OPSEC process is continuous, interactive, and described in detail in reference (b). The elements of the process are:

(1) Identification of CI and its indicators.

(2) Analysis of threats.

(3) Analysis of vulnerabilities.

(4) Assessment of risks.

(5) Application of appropriate countermeasures.

5. Responsibilities

a. OPSEC Officer. The OPSEC Officer is responsible for administering the OPSEC Program per reference (e). The OPSEC Officer should attend all relevant interagency courses (OPSE-2380, OPSE-2390, OPSE-2400, OPSE-3100, and OPSE-3500) offered by the Interagency OPSEC Support Staff (IOSS). Every effort will be made to have Department OPSEC Assistants or working group members attend relevant IOSS courses. Other personnel in the command knowledgeable in areas that affect operations security will assist the OPSEC Officer in the execution of his/her duties. Additional duties of the OPSEC Officer 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) Coordinating the conduct of OPSEC surveys.

(7) Conducting the organization's annual OPSEC assessment per reference (a).

(8) Maintaining a compilation of OPSEC lessons learned.

(9) Coordinating intelligence and counterintelligence support, as necessary.

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

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

(12) Coordinating OPSEC with traditional security program officers.

(13) Coordinating with Navy Public Affairs and OPSEC Officers in support of reference (e).

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

(15)Ensuring command personnel are informed of CI and OPSEC measures are implemented to protect that CI.

(16) Providing guidance to Public Affairs Officers for maintaining operations security.

b. OPSEC Assistants or working group members. OPSEC assistance or working group members will be E-6 or above, assigned from each department and assist the OPSEC Officer in his or her responsibilities. Additional duties include:

(1) Complete the IOSS OPSEC 1301 computer based training.

(2) Attend monthly OPSEC meetings and other meetings scheduled by the OPSEC Officer.

(3) Be actively engaged in annual OPSEC assessments, surveys, 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 Officer will provide relevant reminders during all-hands calls and ensure Plan-of-the-Day/Week (POD/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 Officer will review this instruction annually.

//S//

X. X. XXXXX

Distribution:
XXX
XXX

Figure E-1. Sample Operations Security Instruction

APPENDIX F

Threat Assessment Template

Who is the adversary?			
What is their intent?			
		Proven	Estimated
What is their collection capability? ⇨	SIGINT		
Is the adversary capable of applying this collection ability to action against us?	HUMINT		
☐ Yes ☐ No	OSINT		
	IMINT		
	MASINT		
1. Name a friend of the adversary:			
What are the friends'collection capabilities? ⇨	SIGINT		
Will they share information with the adversary?	HUMINT		
☐ Yes ☐ No	OSINT		
What is this friends' overall threat level?	IMINT		
	MASINT		
2. Name another friend of the adversary:			
What are the friends'collection capabilities? ⇨	SIGINT		
Will they share information with the adversary?	HUMINT		
☐ Yes ☐ No	OSINT		
What is this friends' overall threat level?	IMINT		
	MASINT		
3. Name another friend of the adversary:			
What are the friends'collection capabilities? ⇨	SIGINT		
Will they share information with the adversary?	HUMINT		
☐ Yes ☐ No	OSINT		
What is this friends' overall threat level?	IMINT		
	MASINT		
What is the adversary's overall threat level?			

Figure F-1. Threat Assessment Template

The chart shown above or the chart (reprinted below from Appendix D) may be used for analyzing threats.

Intent		Capability: High	Capability: Medium High	Capability: Medium	Capability: Medium Low	Capability: Low
	Adversary	The Adversary's Collection Capability is HIGHLY developed and MOST LIKELY In place OR The Adversary receives equivalent data collection support from a HIGHLY capable 3rd party	The Adversary's Collection Capability is Significantly developed and PROBABLY In place OR The Adversary receives equivalent data collection support from a SIGNIFICANTLY capable 3rd party	The Adversary's Collection Capability is Possibly developed and LIKELY In place OR The Adversary receives equivalent data collection support from a CAPABLE 3rd party	The Adversary's Collection Capability is PROBABLY NOT developed and MOST LIKELY NOT In place OR The Adversary may receives equivalent data collection support from a 3rd party	The Adversary's Collection Capability is NOT developed OR does NOT receive data from a 3rd party
High	The Adversary is HIGHLY Motivated and a Successful Outcome SIGNIFICANTLY Contributes to Meeting the Adversary's Intended Objectives	High	Medium High	Medium High	Medium	Medium Low
Medium High	The Adversary is SIGNIFICANTLY Motivated and a Successful Outcome GREATLY Contributes to Meeting the Adversary's Intended Objectives	Medium High	Medium High	Medium High	Medium	Low
Medium	The Adversary is SUFFICIENTLY Motivated and a Successful Outcome WILL Contributes to Meeting the Adversary's Intended Objectives	Medium High	Medium	Medium	Medium Low	Low
Medium Low	The Adversary is MODERATELY Motivated and a Successful Outcome CAN Contribute to Meeting the Adversary's Intended Objectives	Medium	Medium Low	Medium Low	Medium Low	Low
Low	The Adversary is NOT Motivated to collect information	Medium Low	Low	Low	Low	Low

Figure D-3 (Reprinted). Threat Matrix

APPENDIX G

Risk Analysis and Countermeasure Considerations

G.1 RISK ASSESSMENT

Risk is assessed as a measure of the probability that an adversary will be successful in collecting CI and the resultant cost to the mission (impact).

1. Probability is determined by multiplying a vulnerability value by the relative threat value. In other words, if the vulnerability involves susceptibility to HUMINT collection, the threat value would be specific to the adversary's HUMINT collection capability. In a situation where a single vulnerability might be exploited by multiple collection methodologies, use the highest rating for risk calculation.

2. Use Figure G-1 as a decision chart for probability, combining the values for threat and vulnerability.

Threat / **Vulnerability**	HI	MED HI	MED	MED LOW	LOW
HI	HI	MED HI	MED	MED LOW	LOW
MED HI	MED HI	MED	MED	MED LOW	LOW
MED	MED	MED	MED	LOW	LOW
MED LOW	MED LOW	MED LOW	LOW	LOW	LOW
LOW	LOW	LOW	LOW	LOW	LOW

Figure G-1. Probability of Critical Information Loss (Threat Severity X Vulnerability Level)

3. Determine the risk by multiplying probability times impact. The measure of impact in this example can be determined by reviewing the value of the CI that is susceptible to HUMINT collection. Should multiple items of CI be susceptible to exploitation by a given vulnerability, the analyst makes a decision on the combined value of that CI. Most often, the combined value is the highest value placed on any one CI item.

4. Use Figure G-2 as a decision chart for risk, combining the values for probability and impact. For example, if the threat is high and the vulnerability is medium high, the probability of compromise is medium high. If the value of the CI is medium high, the risk is medium.

Probability / Impact (CI Value)	HI	MED HI	MED	MED LOW	LOW
HI	HI	MED HI	MED	MED LOW	LOW
MED HI	MED HI	MED	MED	MED LOW	LOW
MED	MED	MED	MED	LOW	LOW
MED LOW	MED LOW	MED LOW	LOW	LOW	LOW
LOW	LOW	LOW	LOW	LOW	LOW

Figure G-2. Risk Assessment

G.2 Countermeasure Consideration

The following contains a countermeasure consideration list that OPSEC officers/planners may find useful in developing their own countermeasures:

1. What is the cost vs. benefit?
2. Do we really need it?
3. Are we creating another 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?

APPENDIX H

Operations Security Assessment Team (or Working Group) 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. Ideally, the assessment team consists of a team leader and team members with expertise in the following function areas (mission/resource dependant):

1. Operations
2. Physical security
3. Computer network operations
4. Administration
5. Supply/logistics
6. Maintenance
7. Communications
8. Foreign disclosure
9. Legal officer
10. Public affairs officer
11. Network security

H.2 TEAM MEMBER RESPONSIBILITIES AND AUTHORITY

Following are general responsibilities of the team:

1. Team leader will:
   a. Brief team members at their initial meeting, covering at a minimum the following items:
      (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) Provide a list of directives and other applicable documents.

b. Organize, coordinate, direct assessment activity (to include interviews), and prepare the OPSEC assessment report.

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

d. Correlate and analyze information acquired by individual team members and through empirical studies (i.e., COMSEC, communications/noncommunications monitoring, etc.); develop recommendations to reduce or eliminate OPSEC weaknesses.

e. Formulate a relevant TA.

f. Provide briefs and comments to correct minor items on the spot to increase OPSEC awareness during the survey.

g. Provide the CO/OIC a verbal completion brief/report, followed by a written, final OPSEC survey report.

2. Team members will:

a. Develop EEFIs, CIs, and other relevant profiles in their respective functional areas.

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

c. Be familiar with other team members' functional areas and be alert for information that may affect them.

d. Conduct interviews; consolidate results.

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

APPENDIX I

Classification Policy for 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, and/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. Certainly there 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 to ensure the information that supports these critical operations is properly safeguarded. Merely classifying information cannot guarantee such safeguards. The proper disclosure of both classified and sensitive unclassified information only to those individuals with appropriate clearance and/or a need-to-know is the strongest protection available.

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, bomb 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 be made only after a risk assessment is completed on the effects such a disclosure would have on the forces involved:

1. Disclosure of a specific date 48 hours in advance of arrival/departure of individual units to/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/departure.

2. Disclosure of a specific date seven days in advance of return/departure of a unit to/from deployment. The advance disclosure time frame (seven 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

Chief of Naval Operations E-Mail and Operations Security Guidance

NAVADMIN 243/01, provided, is Chief of Naval Operations guidance on e-mail and operational security. Commands are reminded to review the latest guidance regarding the use of the internet via NAVADMINs or MARADMINs or other policy guidance.

ADMINISTRATIVE MESSAGE

PRIORITY

P 141837Z SEP 01 ZYB MIN PSN 853669W37

FM CNO WASHINGTON DC//N6//

TO NAVADMIN

UNCLAS//N02000//NAVADMIN 243/01

MSGID/GEN ADMIN/NAVY CIO//

SUBJ/E-MAIL AND OPERATIONAL SECURITY//

REF/A/GENADMIN/CNO WASHINGTON DC/0823 IOZJAN 1999//

REF/B/GENADMIN/CNO WASHINGTON DC/091820ZMAR2001//

REF/C/GENADMIN/CHINFO WASHINGTON DC/301956ZOCT 2000/NOTAL//

NARR/REF A IS NAVADMIN 009/99. ALERTING NAVY PERSONNEL TO THE VULNERABILITIES OF INDISCRIMINATE E-MAIL USAGE. REF B IS NAVADMIN 060/01 PROVIDING AMPLIFYING GUIDANCE FOR NIPRNET USAGE. REF C DISCUSSED MAINTAINING SECURITY AND CLASSIFICATION DURING THE USS COLE INVESTIGATION. REFS A AND B ARE AVAILABLE AT WWW.PERSNET.NAVY.MIL/NAVADMIN/.

RMKS/1. THIS MESSAGE (CIO SERIAL 006-01) REITERATES GUIDANCE PROVIDED FOR THE USE OF UNCLASSIFIED E-MAIL, WEB PAGE CONTENT, AND OTHER INTERNET TOOLS WHICH ARE ACCESSED VIA THE NONSECURE INTERNET PROTOCOL ROUTER NETWORK (NIPRNET) (REFS A AND B GERMANE).

2. E-MAIL COMMUNICATIONS AND WEB USAGE WHICH EMANATE FROM OR VIA GOVERNMENT COMPUTERS, WHETHER BY ORGANIZATION OR INDIVIDUAL, REFLECT DIRECTLY ON THE PROFESSIONALISM OF THE COMMAND AND THE NAVY. ALL HANDS MUST ACT ACCORDINGLY AND ARE CAUTIONED TO REMAIN SENSITIVE TO THE VICTIMS AND THEIR FAMILIES OF THE RECENT ATTACKS IN NEW YORK AND WASHINGTON. WE MUST AVOID THE INADVERTENT

RELEASE OF INFORMATION THAT IS PROPERLY HANDLED BY OUR CASUALTY ASSISTANCE CALLS OFFICES.

3. WHILE NIPRNET/INTERNET E-MAIL AND WEB PAGES USE ARE KEY COMMUNICATIONS TOOLS FOR TODAY'S NAVY, THEIR CONVENIENCE CANNOT REPLACE THE NEED FOR OPERATIONS SECURITY (OPSEC). IT IS ESSENTIAL TO UNDERSTAND:

A. THESE COMMUNICATIONS DO NOT DISAPPEAR LIKE A VERBAL EXCHANGE; B. THEY ARE NOT PRIVATE AND CAN EASILY BE FORWARDED AND MODIFIED BEYOND THE CONTROL OF ANY INDIVIDUAL. E-MAIL AND OTHER ONLINE COMMUNICATIONS SUCH AS CHAT ROOMS AND MESSAGE BOARDS CAN EASILY BE MISINTERPRETED, SPOOFED OR EXPLOITED; C. NIPRNET E-MAIL USAGE IS OFFICIAL GOVERNMENT COMMUNICATIONS AND SUBJECT TO MONITORING, LONG TERM STORAGE, AND POTENTIAL RELEASE UNDER THE FREEDOM OF INFORMATION ACT; D. MOST IMPORTANTLY, INFORMATION RELAYED VIA NIPRNET MUST ONLY BE UNCLASSIFIED.

4. THE FOLLOWING GUIDANCE FROM REF C PROVIDED DURING THE USS COLE INVESTIGATION, REMAINS RELEVANT AND SHOULD BE OBSERVED: INDIVIDUALS PREPARING FORMAL OR INFORMAL ASSESSMENTS OF DAMAGE AND LOSSES, OR THOSE GATHERING AND DISSEMINATING IMAGES OF THE SAME, MUST CAREFULLY CONSIDER AND APPLY APPROPRIATE CLASSIFICATION AND RELEASE INSTRUCTIONS. AREAS OF CONCERN INCLUDE SPECIFIC DAMAGE ASSESSMENTS, SPECIFIC DEGRADATIONS IN CAPABILITIES, OR SPECIFIC PERSONNEL INFORMATION.

5. OPSEC IS A STANDARD AGAINST WHICH ONLINE INFORMATION MUST BE MEASURED. INFORMATION REGARDING NAVY OPERATIONS, FACILITIES, OR PERSONNEL SHOULD ALWAYS BE VIEWED FROM AN OPSEC PERSPECTIVE. THERE IS A CLEAR CONNECTION BETWEEN NIPRNET E-MAIL AND FORCE PROTECTION. DESCRIPTIONS OF EVENTS THAT OCCUR MAY IN THEMSELVES, OR IN CONJUNCTION WITH OTHER INFORMATION, COMPROMISE OPERATIONAL MISSIONS, CAPABILITY DATA, OR DAMAGE ASSESSMENTS. INFORMATION OBTAINED FROM AN OPEN SOURCE MAY IN FACT BE CLASSIFIED AND CITING OR COMMENTING ON IT MAY BE VIEWED AS CONFIRMATION OF THE VALIDITY OF THE OPEN SOURCE DATA. IF IN DOUBT, CONSULT THE CHAIN OF COMMAND AND ERR ON THE SIDE OF CAUTION.

6. COMMANDERS, COMMANDING OFFICERS AND OFFICERS IN CHARGE ARE REQUESTED TO DISSEMINATE THE CONTENTS OF THIS MESSAGE TO ALL HANDS.

7. MINIMIZE CONSIDERED. RELEASED BY VADM R.W. MAYO, USN, NAVY CIO.//

BT

APPENDIX K

Web Site Self-Assessment Checklist

K.1 OVERVIEW

Commands are encouraged to use self-assessment checklists to ensure that CI is absent from public viewing. While conducting self-assessments has no periodicity, each time the Web page is updated with new or additional information, it should be reviewed for content. The NOST at NIOC Norfolk 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. 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. Authorized publicly accessible web presence:

   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. Noncommands are allowed to create a web presence, but only as a sub-web off 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 link to the parent's Web site home page only.

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."

         (a) 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:

            http://www.defenselink.mil/webmasters/policy/dod_web_policy_12071998_with_amendments_and_corrections.html

            and SECNAVINST 5720.47A

http://www.chinfo.navy.mil/navpalib/internet/secnav5720-47a.pdf.

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:

> This is a World Wide Web site for official information about (the name of the command/activity) for the general public.
>
> All information on this site is public domain and may be distributed or copied unless otherwise specified. Use of appropriate byline/photo/image credits is requested.
>
> Unauthorized attempts to upload information or change information on this Web site are strictly prohibited and may be punishable under the Computer Fraud and Abuse Act of 1986 and the National Information Infrastructure Protection Act.
>
> For site security purposes and to ensure that this service remains available to all users, this government computer system employs software programs to monitor network traffic to identify unauthorized attempts to upload or change information, or otherwise cause damage.
>
> Except for authorized law enforcement investigation and to maintain required correspondence files, no other attempts are made to identify individual users or their usage habits. Raw data logs are used to simply determine how many users are accessing the site, which pages are the most popular, and, from time to time, from which top-level domain users are coming. This data is scheduled for regular destruction in accordance with National Archives and Records Administration guidelines.

Figure K-1. 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.

c. Contain a link to parent command or ISIC.

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

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

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

   (1) External links to nongovernment 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—Example:

   "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."

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. Privacy Advisory – Example:

"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 pre-approved 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.

(1) 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).

Notice and Consent Banner Notice – Example:

"This is a Department of Defense Computer System. This computer system, including all related equipment, networks and network devices (specifically including Internet access) are provided only for authorized Government use. DOD computer systems may be monitored for all lawful purposes, including ensuring that their use is authorized, for management of the system, to facilitate protection against unauthorized access and to verify security procedures, survivability, and operational security. Monitoring includes active attacks by authorized DOD entities to test or verify the security of this system. During monitoring, information may be examined, recorded, copied and used for authorized purposes. All information, including personal information, placed or sent over this system may be monitored. Use of this DOD computer system, authorized or unauthorized, constitutes consent to monitoring of this system. Unauthorized use may subject you to criminal prosecution. Evidence of unauthorized use collected during monitoring may be used for administrative, criminal, or other adverse action. Use of this system constitutes consent to monitoring for these purposes."

k. 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.

Any information that can be used to identify DOD individuals. Exception: Command Executives (i.e., CO, XO, CMC) can be identified by photo and name only. The following specific information is not to be divulged:

Social Security Number

Family members

Home address or phone numbers

Birth date or place

Race, religion, citizenship

City home of record

Marital Status

Personalized e-mail address

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 specialized, internal audience or of questionable value to the general public that is not access limited by at least password protection, coupled with 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.chinfo.navy.mil/navpalib/factfile/ffiletop.html for ship characteristics.

INTENTIONALLY BLANK

APPENDIX L

Operations Security Training

L.1 GENERAL

The effective implementation of OPSEC begins with appropriate training. The Navy Training Surface Manual requires that one to two people from each command attend the Navy OPSEC course (J-2G-0966). OPSEC training is essential because at the carrier strike group/expeditionary strike group levels and many shore stations, the duties and responsibilities of the OPSEC officer/planner 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 in their missions, functions, and tasks. It is strongly recommended that every command have, at a minimum, the OPSEC officer receive formal training.

L.2 INTERAGENCY OPERATIONS SECURITY SUPPORT STAFF

The IOSS is located in Greenbelt, MD and is considered the national OPSEC authority. IOSS offers a variety of services to the OPSEC officer/planner, both prospective and current, in the form of OPSEC-related materials and most importantly, training opportunities. Learn more about IOSS at: http://www.ioss.gov. 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 Naval Amphibious Base Little Creek, Norfolk, VA offers a variety of IO-related courses, including the two-day Navy OPSEC course. This course is also offered at the NIOC Detachment, San Diego, CA. It is highly recommended that all OPSEC practitioners attend this class as a prerequisite to follow-on OPSEC training. The course is available via Mobile Team Training upon request.

The Navy OPSEC 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/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. Training includes OPSEC planning as an initial step in all military/operation planning through the development of the OPSEC annex, and developing and instituting OPSEC training for the command or unit. The course provides students with the fundamental knowledge and skills to perform duties as an OPSEC officer/coordinator for a command or unit.

For a complete list of NIOC Norfolk IO courses, including class convening dates and quota information, visit http://www.nioc-norfolk.navy.smil.mil.

L.4 UNITED STATES MARINE CORPS OPERATIONS SECURITY TRAINING

The minimum training requirements for Marine Corps personnel can be found in Marine Corps Order 3070.2.

INTENTIONALLY BLANK

APPENDIX M

Ombudsman/Key Volunteer Network Guidance

M.1 OVERVIEW

Appendix M provides guidance for the command or command representative for discussing OPSEC with the command Navy Ombudsman/Marine Corps KVN and for family OPSEC awareness training during predeployment gatherings and family/spouse support meetings. (Extracts from Chapter 6, which covers OPSEC and the Internet, can help in discussions with the ombudsman/KVN and in OPSEC family awareness meetings.)

M.2 WHAT IS OPERATIONS SECURITY?

Operations Security keeps potential adversaries from discovering our CI. 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 more 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 sent by unfriendly countries to do harm to the United States that make U.S. military efforts fail. Others include individuals or governments that are collecting information that could be used against America in the future, or that could potentially negatively impact mission, morale, and perhaps the American economy. Finally, there are criminals looking for information for personal gain.

Enemies of freedom want our information—all types of information—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 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 recently captured 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 United States and its citizens. Some adversary targets are shown in Figure M-1.

Figure M-1. Adversary Targets

M.4 HOW DOES OPERATIONS SECURITY 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 CI that we urge you to review and protect before, during, and even after your loved one's deployment.

1. Critical information you should protect:

   a. Dates, times, length of deployments, to include departure and arrival dates, using ship's name in correspondence and "Tiger Cruise" information

   b. Places, names, ranks

   c. Numbers of people, parts, or aircraft

   d. En route stop locations

   e. Hotels and room numbers

   f. Personal information, addresses, and family names and addresses

   g. Numbers and names of children

   h. Social security numbers

   i. Bank and credit card information.

2. Other considerations:

   a. Military ID cards indicate you are military affiliated—use your driver's license instead when possible.

   b. Military decals on your vehicle also indicate your military affiliation.

   c. Do not send CI to relatives or others via e-mail, it can be (and is) easily intercepted.

   d. 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!

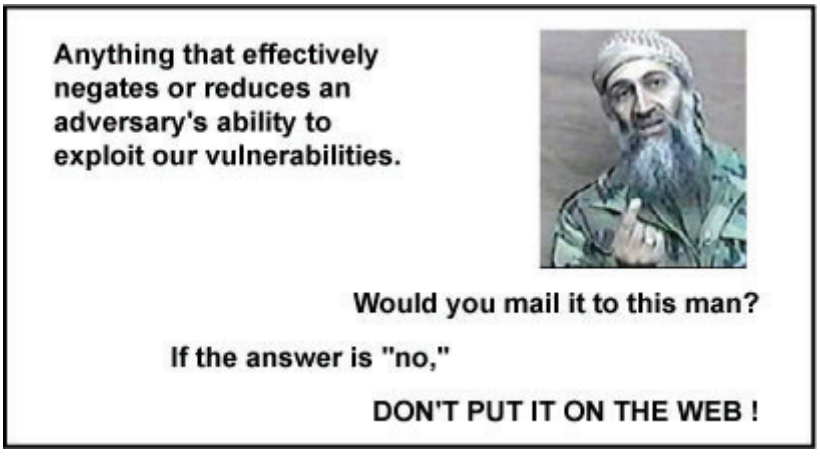

Figure M-2. Diligence in Operations Security

INTENTIONALLY BLANK

APPENDIX N

Sovereign Immunity

N.1 OVERVIEW

Appendix O provides policy established by NAVADMIN 288/05 (CNO WASHINGTON DC 101814ZNOV05) 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 United States 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 United States 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, command officers shall consult with the responsible United States embassy country team and notify their chain of command up to the naval component commander.

INTENTIONALLY BLANK

GLOSSARY

electronic warfare (EW). Military action involving the use of electromagnetic and directed energy to control the electromagnetic spectrum or to attack the enemy. Electronic warfare consists of three divisions: electronic attack, electronic protection, and electronic warfare support. (JP 1-02. Source: JP 3-13.1)

information operations (IO). The integrated employment of the core capabilities of electronic warfare, computer network operations, psychological operations, military deception, and operations security, in concert with specified supporting and related capabilities, to influence, disrupt, corrupt or usurp adversarial human and automated decision making while protecting our own. (JP 1-02. Source: JP 3-13)

military deception (MILDEC). Actions executed to deliberately mislead adversary military decision makers as to friendly military capabilities, intentions, and operations, 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)

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 (OPSEC). A process of identifying critical information and subsequently analyzing friendly actions attendant to military operations and other activities to: a. identify those actions that can be observed by adversary intelligence systems; b. determine indicators that adversary intelligence systems might obtain that could be interpreted or pieced together to derive critical information in time to be useful to adversaries; and c. select and execute measures that eliminate or reduce to an acceptable level the vulnerabilities of friendly actions to adversary exploitation. (JP 1-02. Source: JP 3-13.3)

psychological operations (PSYOP). 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. The purpose of psychological operations is to induce or reinforce foreign attitudes and behavior favorable to the originator's objectives. (JP 1-02. Source: JP 3-53)

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)

INTENTIONALLY BLANK

LIST OF ACRONYMS AND ABBREVIATIONS

AAR	after action report
AIS	automated information system
ALMAR	All Marine
AOR	area of responsibility
AT/FP	antiterrorism/force protection
C2W	command and control warfare
CI	critical information
CJCS	Chairman of the Joint Chiefs of Staff
CNA	computer network attack
CND	computer network defense
CNO	computer network operations
CNOIVA	Chief of Naval Operations installation vulnerability assessment
COMPUSEC	computer security
COMSEC	communications security
DAO	defense attaché offices
DIA	Defense Intelligence Agency
DOD	Department of Defense
DON	Department of the Navy
EEFI	essential elements of friendly information
EMCON	emissions control
EW	electronic warfare
FIS	Foreign Intelligence Services
FOUO	for official use only
FP	force protection

HUMINT	human intelligence
IMINT	imagery intelligence
INFOSEC	information security
IO	information operations
IOSS	Interagency OPSEC Support Staff
ISIC	immediate superior in command
KVN	Key Volunteer Network
LAN	local area networks
LOGREQ	logistic request
MAA	master-at-arms
MASINT	measurement and signature intelligence
MCO	Marine Corps order
MILDEC	military deception
MILSTRIP	military standard requisitioning and issue procedure
MTAC	Multiple Threat Alert Center
NCDOC	Navy Cyber Defense Operations Command
NCIS	Naval Criminal Investigative Service
NIOC	Navy Information Operations Command
NIPRNET	Non-Secure Internet Protocol Router Network
NOST	Naval OPSEC Support Team
NSDD	national security decision directive
NTTP	Navy tactics, techniques, and procedures
OCE	officer conducting the exercise
OLS	online survey
OPORD	operation order
OPSEC	operations security
OSCAR	operations security collaboration architecture
OSINT	open-source intelligence

PA	public affairs
PAO	public affairs officer
POD	print on demand
PSYOP	psychological operations
ROE	rules of engagement
SIGINT	signals intelligence
SIPRNET	SECRET Internet Protocol Router Network
SOP	standard operating procedure
SOPA	senior officer present afloat
TA	threat assessment
UNCLAS	unclassified
U.S.	United States
USPACOM	United States Pacific Command
WWW	World Wide Web

INTENTIONALLY BLANK

LIST OF EFFECTIVE PAGES

Effective Pages	Page Numbers
MAR 2009	1 thru 18
MAR 2009	1-1, 1-2
MAR 2009	2-1 thru 2-4
MAR 2009	3-1 thru 3-6
MAR 2009	4-1 thru 4-6
MAR 2009	5-1, 5-2
MAR 2009	6-1 thru 6-6
MAR 2009	7-1, 7-2
MAR 2009	8-1, 8-2
MAR 2009	9-1, 9-2
MAR 2009	10-1 thru 10-4
MAR 2009	A-1 thru A-8
MAR 2009	B-1, B-2
MAR 2009	C-1 thru C-6
MAR 2009	D-1 thru D-8
MAR 2009	E-1 thru E-4
MAR 2009	F-1, F-2
MAR 2009	G-1, G-2
MAR 2009	H-1, H-2
MAR 2009	I-1, I-2
MAR 2009	J-1, J-2
MAR 2009	K-1 thru K-6
MAR 2009	L-1, L-2
MAR 2009	M-1 thru M-4
MAR 2009	N-1, N-2
MAR 2009	Glossary-1, Glossary-2
MAR 2009	LOAA-1 thru LOAA-4
MAR 2009	LEP-1, LEP-2

INTENTIONALLY BLANK

NTTP 3-54M/MCWP 3-40.9
MAR 2009