NAVY TACTICS, TECHNIQUES, AND PROCEDURES

OPERATIONS SECURITY
NTTP 3-13.3

EDITION DECEMBER 2022

DEPARTMENT OF THE NAVY
OFFICE OF THE CHIEF OF NAVAL OPERATIONS

DISTRIBUTION/DISSEMINATION CONTROL:
APPROVED FOR PUBLIC RELEASE; DISTRIBUTION IS UNLIMITED
POC: NIWDC_N5@NAVY.MIL

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

PRIMARY REVIEW AUTHORITY:
NAVAL INFORMATION WARFIGHTING DEVELOPMENT CENTER

RECORD OF CHANGES		
NUMBER	DATE	ENTERED BY

This and other Navy Warfare Library publications, including any edition updates, are available at the Navy Warfare Library websites: https://doctrine.navy.mil/ and https://doctrine.navy.smil.mil/.

DEPARTMENT OF THE NAVY
NAVAL INFORMATION WARFIGHTING DEVELOPMENT CENTER
7941 BLANDY ROAD SUITE 500
NORFOLK VA 23551-2403

3510
Ser N5/212
16 Dec 22

LETTER OF APPROVAL

1. NTTP 3-13.3 (DEC 2022), Operations Security, is hereby approved.

2. NTTP 3-13.3 provides tactics, techniques, and procedures to assist the operations security (OPSEC) officer and commander in identifying critical information and applying OPSEC considerations in mission planning and day-to-day activities.

3. NTTP 3-13.3 was developed per NTRP 1-01 (June 2021), The Navy Warfare Library User Manual, and supersedes NTTP 3-13.3M (SEP 2017), Operations Security. Destroy superseded materials per DoDM 5200.01, Volume 3, Department of Defense Information Security Program: Protection of Classified Information.

4. NTTP 3-13.3 is unclassified and approved for public release. Distribution is unlimited.

B. E. BRASWELL
Commander
Naval Information Warfighting Development
Center

NTTP 3-13.3 (DEC 2022), Operations Security, is promulgated as a doctrinal publication in the Navy Warfare Library.

Michael R. Durkin

MICHAEL R. DURKIN
Senior Executive Service, U.S. Navy
Director
Navy Warfare Development Center

CONTENTS

Page
No.

CHAPTER 1—INTRODUCTION

CHAPTER 2—OPERATIONS SECURITY

CHAPTER 3—OPERATIONS SECURITY CYCLE

CHAPTER 4—ASSESSMENTS

CHAPTER 5—OPERATIONS SECURITY IN MESSAGES

Page
No.

CHAPTER 6—OPERATIONS SECURITY PLANNING

APPENDIX A—IDENTIFY CRITICAL INFORMATION AND INDICATORS

APPENDIX B—THREAT AND VULNERABILITY ANALYSIS

APPENDIX C—RISK ASSESSMENT AND COUNTERMEASURE CONSIDERATIONS

APPENDIX D—INTERNAL ASSESSMENT PROCEDURES

APPENDIX E—OPERATIONS PLAN/ORDER EXAMPLE

APPENDIX F—COMMAND AND UNIT MOVEMENTS

APPENDIX G—ACQUISITIONS AND CONTRACTS

Page
No.

LIST OF ILLUSTRATIONS

Page No.

CHAPTER 2—OPERATIONS SECURITY

CHAPTER 3—OPERATIONS SECURITY CYCLE

CHAPTER 4—ASSESSMENTS

CHAPTER 5—OPERATIONS SECURITY IN MESSAGES

CHAPTER 6—OPERATIONS SECURITY PLANNING

APPENDIX A—IDENTIFY CRITICAL INFORMATION AND INDICATORS

APPENDIX B—THREAT AND VULNERABILITY ANALYSIS

Page
No.

APPENDIX C—RISK ASSESSMENT AND COUNTERMEASURE CONSIDERATIONS

APPENDIX D—INTERNAL ASSESSMENT PROCEDURES

APPENDIX E—OPERATIONS PLAN/ORDER EXAMPLE

APPENDIX G—ACQUISITIONS AND CONTRACTS

APPENDIX H—OPERATIONS SECURITY PUBLIC RELEASE REVIEW

INTENTIONALLY BLANK

PREFACE

NTTP 3-13.3 (DEC 2022), OPERATIONS SECURITY, is available in the Navy Warfare Library (NWL). It is effective upon receipt and supersedes NTTP 3-13.3M (SEP 2017), OPERATIONS SECURITY.

NTTP 3-13.3 is the Department of the Navy comprehensive operations security (OPSEC) guide providing OPSEC officers and commanders with methods for incorporating OPSEC into daily activities, exercises, and mission planning.

INSTRUCTIONS FOR USE

This and other Navy Warfare Library publications, including edition updates, are available on the NWL portal (https://doctrine.navy.mil/ or https://doctrine.navy.smil.mil/). Printed copies may be ordered by following the directions included in Appendix A of NTRP 1-01, The Navy Warfare Library User Manual.

Report urgent changes, routine changes, and administrative discrepancies by letter, general administrative message, or email to NAVY WARFARE DEVELOPMENT CENTER, ATTN: DOCTRINE, 1528 PIERSEY STREET, BLDG O-27, NORFOLK, VA 23511-2723. (Email: NWDC_NRFK_FLEET_PUBS@NAVY.MIL)

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” and “must” indicate 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.

INTENTIONALLY BLANK

CHAPTER 1
Introduction

1.1 PURPOSE

Operations security (OPSEC) enables mission success by identifying and protecting sensitive unclassified information. This publication is the United States Navy's comprehensive OPSEC guide, providing OPSEC officers and commanders with methods for incorporating OPSEC into daily activities, exercises, and mission planning.

1.2 SCOPE

This publication covers the Department of Defense (DOD) OPSEC cycle, OPSEC assessments, and the OPSEC planning process. Additional information includes the role of OPSEC in force protection, the role of the United States (U.S.) intelligence community in OPSEC, and OPSEC considerations in the acquisition process and contracts. It provides tactics, techniques, and procedures (TTP) to assist the OPSEC officer, and ultimately commanders, in identifying critical information and applying OPSEC considerations in mission planning and day-to-day activities.

> Operations security as a concept is probably as old as war itself. Nevertheless, the fact that poor OPSEC practices have been costly in loss of human life and lost objectives in every American war demonstrates that, despite its venerated age, operations security as a doctrine needs to be learned afresh by each generation.
>
> *Center for Cryptologic History, 1993*
> *PURPLE DRAGON: The Origin and Development of the United States OPSEC Program*

1.3 BACKGROUND

SECNAVINST 3070.2A, Operations Security, serves as the foundation for this publication and incorporates lessons learned over many years of naval OPSEC and addresses emerging areas, such as the use of social media.

INTENTIONALLY BLANK

CHAPTER 2
Operations Security

2.1 OVERVIEW

OPSEC is a capability that identifies and controls critical information and indicators (CII) of friendly force actions attendant to military operations and reduces the risk the adversary can exploit friendly force vulnerabilities by incorporating OPSEC measures and countermeasures. When effectively employed, it denies or mitigates the 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, the adversary can forecast, frustrate, or defeat major military operations. OPSEC assists in blinding the adversary, forcing them to make decisions with insufficient information.

OPSEC is an information-related capability (IRC) that, when properly employed, can be used to gain advantages in the information environment (IE), just as other military techniques are used in the operational environment (OE). OPSEC mutually supports other IRCs, such as military deception (MILDEC), public affairs (PA), and cyberspace operations. When effectively integrated, OPSEC and other IRCs can create the operational conditions necessary to achieve the commander's objectives. Figure 2-1 depicts the characteristics of OPSEC.

OPSEC…

1. Is an analytic process
2. Focuses on adversary collection capability and intent
3. Emphasizes the value of critical information
4. Is an information related capability.

Figure 2-1. Operations Security Characteristics

Every Navy command performs missions, tasks, and functions that expose unclassified information and indicators. Indicators are friendly actions and open-source information that the adversary's intelligence system can potentially detect, obtain, and then interpret to derive friendly force critical information.

Individual indicators, when pieced together with other unclassified information, can reveal classified or critical information. The adversary can use this disclosed information to take actions to jeopardize friendly force missions. Data aggregation is the process of piecing such information and indicators together (see Figure 2-2).

The OPSEC cycle provides a means for screening information prior to its release in order to prevent the aggregation of information, ultimately preventing the disclosure of friendly force intentions, capabilities, or other aspects of an operation. Aggregation of information with its potentially negative impact on an operation, mission, activity, and personnel safety is a fundamental OPSEC concept.

> 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 George Washington*

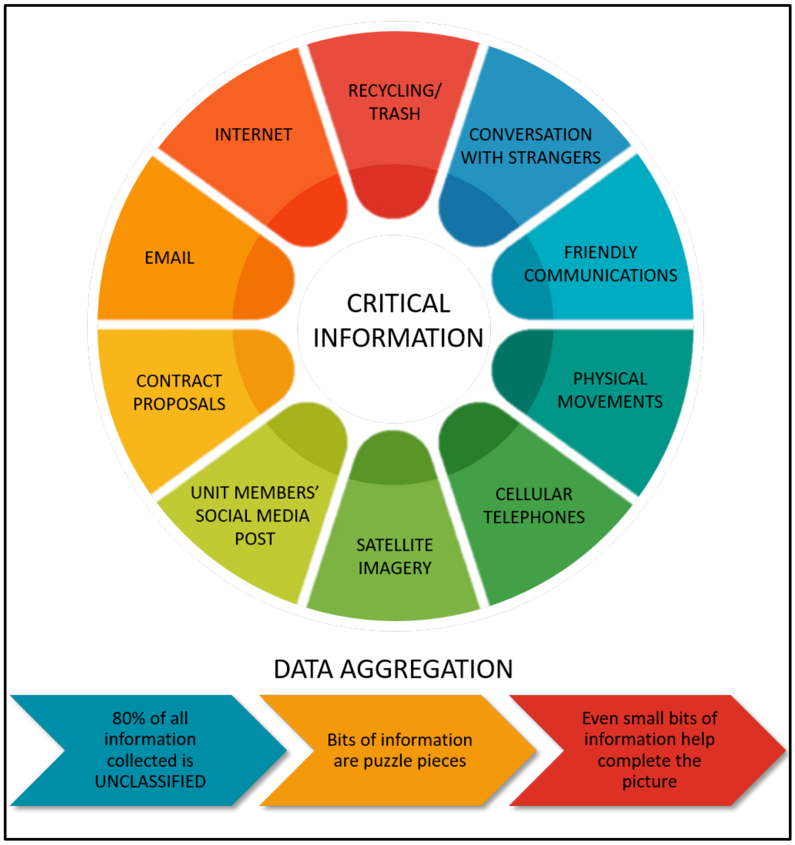

RECYCLING/ TRASH
CONVERSATION WITH STRANGERS
FRIENDLY COMMUNICATIONS
PHYSICAL MOVEMENTS
CELLULAR TELEPHONES
SATELLITE IMAGERY
UNIT MEMBERS' SOCIAL MEDIA POST
CONTRACT PROPOSALS
EMAIL
INTERNET
CRITICAL INFORMATION
DATA AGGREGATION
80% of all information collected is UNCLASSIFIED
Bits of information are puzzle pieces
Even small bits of information help complete the picture

Figure 2-2. Data Aggregation

It is incumbent upon commanders to incorporate OPSEC into all operations. An effective OPSEC program has the chain of command's full support. Command emphasis includes the appointment of an OPSEC officer or coordinator in writing by the commanding officer, and the establishment of an operations security working group (OWG) charged with ensuring the command and associated family members maintain acute OPSEC awareness.

While not a remedy for every operational challenge, OPSEC measures/countermeasures, if enacted properly, can minimize the risk of compromising information that could aid the adversary in degrading friendly force mission effectiveness.

2.2 CHARACTERISTICS OF OPERATIONS SECURITY

OPSEC is a dynamic process and can change as the mission and environment changes. Information critical in one phase of a mission, may not be critical in subsequent phases. The threat faced in one situation, may be different in the next. Vulnerabilities in one situation, may not exist in another. Risks may vary as information criticality, threats, and vulnerabilities change independently and in relation to one another. Operations security measures/countermeasures that are effective in a specific situation, may not work in other situations. Deception, a critical OPSEC countermeasure, rarely works against a specific adversary more than once.

OPSEC is an operation enabler that is best incorporated at the start of an operation or mission planning, not added on as an afterthought. The OPSEC cycle allows for the integration and mutual support of all traditional security disciplines (e.g., physical, information, cyber, personnel, and technical) and links to other IRCs and operational functions (e.g., maneuver, logistics, and intelligence). OPSEC denies the adversary the ability to observe or interpret friendly force indicators and disrupts the adversary's collection of information that is generally unclassified. It does not replace traditional security programs created to protect classified information.

OPSEC is an operations function. Security, intelligence, counterintelligence (CI) and other functions and capabilities support its implementation. OPSEC officers use expertise gained through formal training and must possess an understanding of the mission and OPSEC cycle in order to choose the best course of action (COA) to protect critical information.

OPSEC is a command responsibility. The entire command and associated family members participate in the execution of OPSEC measures. The command trains, plans, and executes OPSEC for every activity, exercise, and mission. It requires, at a minimum, OPSEC-trained officers capable of coordinating functions for the commander and advising the commander on the OPSEC cycle, best practices, and implementation as part of a risk-management decision cycle.

2.3 EVOLUTION OF OPERATIONS SECURITY

> In the lead up to Russia's invasion of Ukraine in February 2022, the Chairman of the Joint Chiefs of Staff General Mark A. Milley said, there were "young people in their 20s, running around with iPhones, collecting and sharing videos of Russian forces massing on the Ukrainian border. Those weren't spies—Ukrainian spies, American spies, French or British spies. Those were just citizens out there with cameras taking videos of Russian mechanized vehicles, infantry fighting vehicles and tanks, driving down roads, going to assembly areas, etc."
>
> The ubiquity of sensed information, often emerging directly from people's phones onto social media, makes every target easier to see and hit. All this information made it easy to deduce Russia's intent, the size of its force, and its possible attack routes. In a world of ubiquitous sensors, militaries must move away from large, conspicuous force deployments toward smaller units that change location rapidly and don't attract notice.
>
> "Your concealment, the size of your force, and the speed at which you move around a battlefield will contribute directly to your survivability on a future battlefield that is highly lethal."
>
> *General Mark Milley*

Introduction of the term OPSEC and the creation of the DOD OPSEC program occurred in the late 1960s, having its origins in Operation PURPLE DRAGON during the Vietnam War. However, the concept has been around as long as the practice of warfare. OPSEC has been a fundamental element in virtually all warfare throughout recorded history and remains a key element to achieve strategic and tactical surprise. Evidence can be found of OPSEC principles dating back to the earliest operations of the U.S. military.

> On the banks of the Delaware River in December 1776, General George Washington set in motion one of the great surprise attacks in military annals. Receiving intelligence that the British forces had entered winter quarters, Washington began planning for a surprise attack on the Hessian garrison in Trenton, NJ. Practicing sound OPSEC, Washington set pickets to prevent British forces from observing his preparations and issued orders prohibiting American forces from crossing the river to prevent tipping off the enemy. Preparations culminated the night of December 25th, when General Washington secretly ferried the American forces across the Delaware River and marched 10 miles under the cover of darkness, securing every person they came across to maintain secrecy. On the morning of December 26th, the Americans surprised the Hessian garrison and won a decisive victory. The importance Washington placed on OPSEC prevented the enemy from strengthening their defenses while the Continental Army prepared and executed the operation.
>
> *Center for Cryptologic History, 1993*
> *PURPLE DRAGON: The Origin and Development of the United States OPSEC Program*

World War II (WWII) demonstrated an awareness that OPSEC measures need to address more than just military vulnerabilities. A holistic approach to OPSEC was evident in the planning for Operation OVERLORD during WWII. The operation plans (OPLANs) for the invasion at Normandy included the expected military measures, but also added measures affecting the public. In order to protect OPSEC, the plan restricted civilian international travel between Britain and Ireland, banned visitors within 10 miles of sensitive coastal areas, and restricted transatlantic telephone, cable, and radio communications to prevent intercept and inadvertent spillage. These and other measures executed before and during the invasion were coordinated with an elaborate deception plan to confuse the enemy and created the secure environment needed to mount Operation OVERLORD.

> Every precaution was taken against leakage of our true operational intentions against Normandy. The highest degree of secrecy was maintained throughout all military establishments, both British and American, but additional broader measures affecting the general public were necessary as D-Day approached.
>
> *General Dwight D. Eisenhower*
> *Supreme Allied Commander of the Allied Expeditionary Force*

The origin of the OPSEC program started during the Vietnam War in response to evidence that the North Vietnamese were putting together seemingly unrelated unclassified information to predict and prepare for U.S. bombing missions. The U.S. response was Operation PURPLE DRAGON.

Operation PURPLE DRAGON sought to find the sources of leaked classified information. Operation PURPLE DRAGON teams put themselves in the position of the adversary and developed a complete overview of each mission and operation. The teams began by reviewing operation orders (OPORDs) and directives, communication-electronics operating instructions, pertinent communications security (COMSEC), and other documentation to familiarize themselves with the mission and operation before commencing their analysis. Their focus was on the small, seemingly insignificant details. Their findings revealed the adversary could piece together a variety of small, seemingly insignificant details from unclassified planning products, messages, and documents to predict U.S. targets. The success of Operation PURPLE DRAGON and subsequent OPSEC studies continued to search out the compromise of critical information and provided viable countermeasures to enemy threats.

> In late 1965, the National Security Agency (NSA) uncovered evidence of North Vietnamese early waring alerts to ARC LIGHT bombing missions. Following the implementation of Operation PURPLE DRAGON recommendations, enemy early warning alerts of B-52 strikes dropped significantly. During December 1966, the first month of Operation PURPLE DRAGON survey, two North Vietnamese Army (NVA) stations had early warning for 34 percent of ARC LIGHT missions with an average warning time of eight and a half hours. In April 1967, at the end of Operation PURPLE DRAGON, the NVA's alert broadcasts had fallen to only five percent, with an average alert time of less than 30 minutes.
>
> *Center for Cryptologic History, 1993*
> *PURPLE DRAGON: The Origin and Development of the United States OPSEC Program*

In May 1968, the success of Operation PURPLE DRAGON led General Earle Wheeler, the Chairman of the Joint Chiefs of Staff, to direct all unified and specified commands to establish OPSEC programs. In 1988, these programs expanded to cover government agencies outside of the DOD when President Ronald Reagan issued NSDD 298, National Operations Security Program, which established the national OPSEC policy. The DOD OPSEC program has continued to evolve with adversary capabilities and the availability of new technology.
In 2005, the DOD established the OPSEC support elements in each Service and the joint force to better manage the OPSEC program, conduct OPSEC assessments, and provide training, planning, and exercise support. In 2012, a follow-on educational needs assessment identified gaps in the integration of OPSEC during operational planning, leading to the development of the Defense Operations Security Planners Course (DOPC) to enhance OPSEC planning across the joint force.

As the proliferation of exploitable technologies (e.g., the advent of the internet, mobile devices, and social media) grows, commanders, OPSEC planners, and individual warfighters must be more sensitive than ever to OPSEC vulnerabilities.

> In 2017, the fitness-tracking application Strava released a map detailing all location data uploaded by its users, including U.S. and foreign service members. When visualized as a heat map and cross-referenced with a mapping application the activities highlighted locations potentially related to U.S. military forward operating bases in Afghanistan, Turkish military patrols in Syria, and a possible guard patrol in the Russian operating area of Syria.
>
> *Hern, Alex. The Guardian, January 28, 2018*
> *Fitness Tracking App Strava Gives Away Location of Secret US Army Bases*

For individual warfighters and their families, the choice of security settings on their phones and other connected devices can determine to what extent their habits are trackable, traceable, and predictable.

> Instead of gunfire or artillery explosions, some of the first signs that Russia was invading Ukraine on February 24, 2022, came from Twitter. Experts compiled open-source traffic data from Google and shared the first indications of Russian troop movements in real time on Twitter. The world watched as Twitter exploded with real-time data, reporting, and analysis of the unfolding conflict. It quickly became clear that the war presented analysts with an unprecedented amount of rich, open-source data on military movements, troop location, shelling damage, weapon types, and more. Their analysis and reporting emerged as a critical resource on the conflict, providing combatants and observers with incredible insight and minute-by-minute assessments of what was happening on the ground. Ukraine was quick to capitalize on Russia’s inability to protect open-source data and exploited this weakness to track and impede ongoing Russian military operations.
>
> *Smith, Maggie & Stark, Nick. The Modern War Institute at West Point, May 24, 2022*
> *Open-Source Data Is Everywhere—Except The Army’s Concept Of Information Advantage*

Sailors operating in the modern information environment continue to face many challenges from the proliferation of overhead sensors, small commercial drones, and internet of things technologies. Artificial intelligence and machine-learning algorithms make data aggregation faster and more efficient, linking big data together like never before, and making it increasingly difficult to be unobserved. Commanders must utilize OPSEC to mitigate these complex vulnerabilities to achieve desired effects at the time of their choosing to maintain essential secrecy.

INTENTIONALLY BLANK

CHAPTER 3

Operations Security Cycle

The protection of essential operational aspects and subsequently critical information is fundamental to operational and mission success. Failure to identify operational aspects and critical information renders a commander ineffective in mitigating operational- and mission-related vulnerabilities and inhibits the commander's ability to conduct risk assessments and enact appropriate measures/countermeasures against adversary threats. The OPSEC cycle is the enabling vehicle for OPSEC analysis and the employment of measures/countermeasures. This chapter provides guidance on how to conduct effective OPSEC analysis to support an OPSEC program. Figure 3-1 depicts the OPSEC cycle.

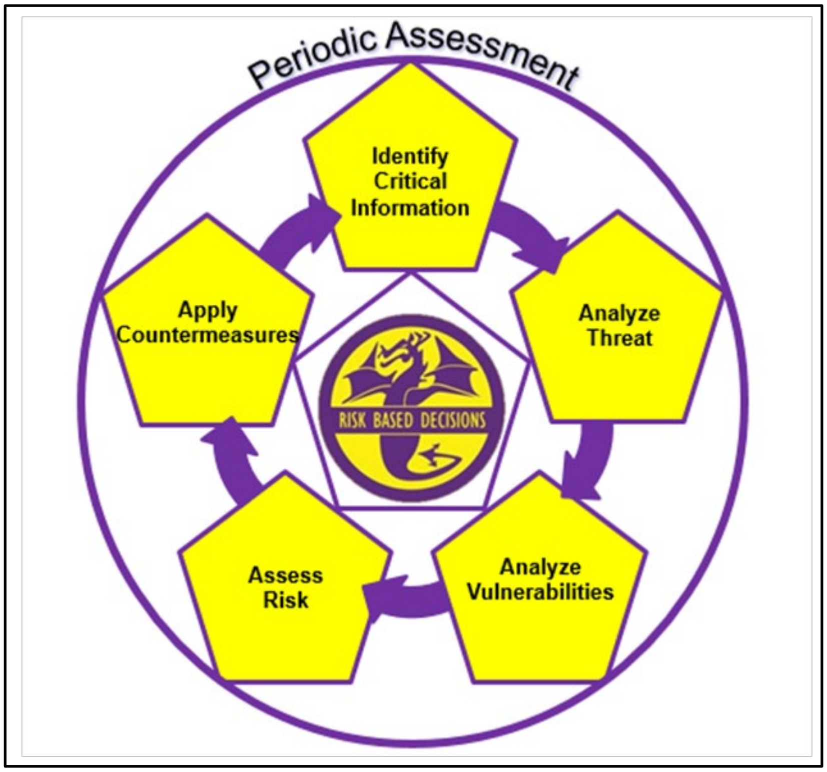


Figure 3-1. The Operations Security Cycle

Immediate superior in command (ISIC) OPSEC officers provide OPSEC program and planning guidance to their subordinate units to ensure all units operate under the same principles for a given area of operations (AO). All units must adhere to higher command guidelines to maximize OPSEC effectiveness. OPSEC analysis must be closely coordinated with other operational planning efforts. Applying OPSEC during the planning phase of any event or activity greatly enhances the commander's ability to identify and protect critical information and maintain essential secrecy.

3.1 OPERATIONAL ASPECTS (ESSENTIAL SECRETS)

The successful application of the OPSEC cycle depends upon the detailed and accurate identification of mission-related critical information. Since critical information is unique to the mission, compiling a single list of critical information for the Navy is impractical. However, it is feasible to identify the operational aspects pertinent to a command and its mission giving the commander and OPSEC officer the flexibility to develop a command- or mission-level critical information list (CIL).

OPSEC officers identify the operational aspects that apply to an operation or planned event. Operational aspects become the essential secrets withheld from the adversary to achieve mission success. The operational aspects include presence, capability, strength, intent, readiness, timing, location, and method. Not all operational aspects are applicable to all activities. Figure 3-2 provides a description of each operational aspect.

Operational Aspects
Presence is the current physical or virtual placement of a unit, tool, or capability within the OE. The adversary might desire to know which units exist in a specific environment and which units do not. This information can become particularly useful when coupled with information about the unit's strength, capability, or intent. When viewed in context, the presence of a unit in an environment can also indicate intent, method, or timing. Although a unit's presence may be difficult to conceal, OPSEC officers must consider how the adversary can use presence when viewed within the context of the rest of the IE.
Capability is the resources or functions that enable the execution of a particular kind of military action. Closely related to the strength aspect of an operation, the capability aspect describes what type of actions a particular unit can execute. OPSEC officers must note that different units have different functions and capabilities. The mere presence of a specific unit in the OE may reveal specific capabilities of the military force.
Strength is the aspect of friendly activities that describes the capacity to carry out a capability. Though this aspect is similar to readiness and capability, it deals more with force levels. One can consider it a percentage of strength compared with the level necessary to carry out a specific task or function. To OPSEC officers, strength is important to consider because the adversary can determine how much of a function the military force can bring to bear in the OE.
Intent is what a military force can do and the conditions the force must establish to accomplish the mission. This closely relates to the commander's end state. The adversary can understand the very nature and purpose of a military force's mission by understanding the intent.
Readiness is the ability of a military force to fight and meet the demands of an assigned mission. OPSEC officers consider how quickly a military force can bring its assets to bear in the OE. If the adversary can determine friendly forces' readiness, they may be able to determine how quickly they can respond to friendly force actions.
Timing is the when, or chronological sequence of actions. Disclosure of timing can be especially damaging to a mission or plan because it can reveal to the adversary when specific actions are to take place in the OE. This allows the adversary to plan activities around friendly force planned operations or missions. OPSEC officers must carefully assess how to protect timing and the cost it can have to a bigger plan.
Location is the projected physical or virtual position where a friendly force acts to achieve a desired effect. Although this aspect is simple in nature, it is of extreme value to the adversary.
Method is how friendly forces accomplish the intended objective—the operational approach to the mission. If the adversary correctly pieces together the friendly force method for achieving an objective, they may develop a plan to seize the initiative at multiple points along the friendly force line of effort. OPSEC officers usually focus heavily on protecting the method of a plan, operation, or mission.

Figure 3-2. Operational Aspects

3.2 CRITICAL INFORMATION AND INDICATORS IDENTIFICATION

Critical information is information about friendly (i.e., U.S., allied, or coalition) activities, that the adversary seeks to act effectively against. Such information, if revealed to the adversary, may prevent or complicate mission accomplishment, reduce mission effectiveness, damage friendly force resources, or cause loss of life. Critical information usually involves a few key elements of information concerning friendly activities or intentions that, if revealed to the adversary, may significantly degrade mission effectiveness. However, information determined to be critical in one phase of an operation or activity, may not be critical in all phases. Critical information should be derived from identified operational aspects. Critical information includes only vital information the adversary needs to plan against and disrupt friendly force operations. Identifying critical information focuses the remainder of the OPSEC cycle on protecting the critical information, rather than attempting to protect all information.

Indicators are friendly detectable actions and open-source information that can be interpreted or pieced together to allow the adversary to obtain critical information or to identify friendly force vulnerabilities. Indicators, when considered with critical information, provide a more comprehensive picture of potential vulnerabilities. There are five major characteristics of an OPSEC indicator—signatures, associations, profiles, contrasts, and exposure (SAPCE). Figure 3-3 provides a description of each OPSEC indicator.

Indicator Characteristics
Signatures are a characteristic of an indicator that makes it identifiable or causes it to stand out. It is usually unique and stable. Adversary intelligence entities key into uncommon signatures that reduce ambiguity in their intelligence assessments, allowing the adversary to anticipate future actions.
Associations are relationships of an indicator to other information or activities. It is an important factor in the adversary's interpretation of an activity.
Profiles of activity are the summation of all signatures and associations. Each friendly force activity generates its own unique profile. Over time, the adversary observes these profiles and builds a baseline to measure changes or deviations.
Contrasts are the changes and deviations from a standard profile. Even when not fully understood, these changes attract interest from adversary intelligence analysts and may lead to more focused collection efforts. Observing contrasts is one of the most reliable means of detecting friendly force activity.
Exposure of an indicator is a characteristic that refers to when and how long an indicator is observable. The duration, repetition, and timing of an indicator's exposure can affect its relative importance and meaning.

Figure 3-3. Indicator Characteristics

Linkages exist between operational aspects, critical information, and indicators. Compromise of the essential secrecy of an operation or mission may occur as the adversary observes indicators of a friendly force activity, critical information, and operational aspects. Appendix A provides additional guidance on determining unit-specific CII.

3.3 THREAT ANALYSIS

Current, accurate, and relevant threat information is critical in developing appropriate operations security measures/countermeasures. Analyzing a threat in the OPSEC cycle includes identifying potential adversaries in the OE, and their associated capabilities, limitations, and intentions to collect, analyze, and use critical information against friendly forces.

Understanding the value of critical information to the adversary helps clarify the lengths to which the adversary would go to acquire it. Many joint, interagency, CI, and intelligence organizations (e.g., Naval Criminal Investigative Service (NCIS), Defense Intelligence Agency, Federal Bureau of Investigation, and local law enforcement authorities) can provide detailed information about the adversary's past, current, and projected operational and intelligence collection capabilities. OPSEC officers can submit a request for information (RFI) to an intelligence entity/agency to gain specific intelligence about the adversary. Example RFIs include:

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

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

3. What is the adversary's possible COA for opposing the friendly force planned operations?

4. What critical information does the adversary already have about the operation?

5. What are the adversary's intelligence collection capabilities (e.g., human intelligence (HUMINT), signals intelligence (SIGINT), open-source intelligence (OSINT), geospatial intelligence (GEOINT), and measurement and signature intelligence (MASINT))?

Appendix B provides more information on evaluating threat information during the OPSEC cycle.

3.4 VULNERABILITY ANALYSIS

Identifying friendly force vulnerabilities is one of the primary reasons the DOD and Navy require all organizations to conduct annual assessments and maintain a culture of OPSEC awareness.

An operation- or mission-related vulnerability exists when the adversary has the capability to collect indicators, correctly analyze them, and take timely action to exploit friendly force operations or missions. Weaknesses reveal CII that, when collected and analyzed by the adversary, create vulnerabilities.

To begin a vulnerability analysis, OPSEC officers communicate with other security elements in the organization (e.g., CI, physical security, industrial security, cybersecurity, and COMSEC). These security elements participate in the OWG. Both OPSEC and traditional security elements seek to deny access of valuable information to the adversary by different, yet complimentary approaches. For example, COMSEC efforts focus on limiting exploitation of specific communications, while cybersecurity efforts identify computer systems and networks containing critical information requiring protection. Traditional security planners can provide valuable inputs to help identify CII. OPSEC officers evaluate the criticality of the identified vulnerabilities based on the impact to friendly force operations. These vulnerabilities could allow direct access to, or possibly reveal, essential secrets to the adversary. Examples of common vulnerabilities include:

1. Lack of awareness or apathy to security procedures

2. Lack of policy enforcement

3. Social media, geolocation enabled devices, and other technologies

4. Unsecured communications

5. Improper disposal of trash.

Indicators require some level of analysis for the adversary to derive friendly force vulnerabilities. OPSEC officers evaluate identified indicators based on the following considerations:

1. Which indicators can the adversary observe through their collection capabilities?

2. Can the adversary analyze the information, make a decision, and take appropriate action in time to interfere with the planned operation?

3. What is the potential impact to the operation or activity if the adversary acts?

Examples of indicators that could expose friendly force vulnerabilities include:

1. Increasing physical or administrative security around a particular project

2. Requesting maps or information on particular geographical areas

3. Filing flight plans or requesting diplomatic clearances

4. Repeating an observable function the same way, allowing the adversary to predict future actions or activity.

3.5 RISK ASSESSMENT

OPSEC officers provide risk assessments to the commanding officer after analyzing friendly force vulnerabilities and assessing the impact those vulnerabilities could have on the mission, operation, or command, if left unmitigated. Risk assessments estimate the adversary's capability to exploit a vulnerability and the potential effects such exploitation could have on an operation. They provide a cost-benefit analysis of mitigating or eliminating the vulnerability. Successful implementation of OPSEC requires managing all dimensions of risk to maximize mission effectiveness and sustain readiness. Applying operational risk management enables the commander to avoid unnecessary risk and accept necessary risk when the cost of mitigation outweighs the benefit. Appendix C contains a risk assessment worksheet and an example of risk assessment rating criteria. Effective use of these tools greatly enhances an organization's OPSEC posture.

3.6 MEASURE/COUNTERMEASURE APPLICATION

OPSEC measures/countermeasures mitigate vulnerabilities in order to preserve military capabilities from adversarial exploitation. The three general goals of OPSEC measures/countermeasures are to:

1. Prevent the adversary from detecting an indicator. A primary OPSEC goal is to mask or control friendly force actions to prevent the collection of critical information or indicators. This includes using protective measures to create closed information systems, signature management, and cryptographic protection and standardized security procedures.

2. Provide alternative deceptive interpretations of an indicator. Preventing the adversary from detecting an indicator may not be possible or cost effective. These circumstances may require attempts to disrupt or confuse the adversary's ability to interpret the indicator. In this situation, the use of tactical deception or deception in support of operations security (DISO) may be appropriate. DISO is a military deception activity that protects friendly operations, personnel, programs, plans, capabilities, equipment, and other assets against adversary collection.

3. Attack the adversary's collection system. Eliminate or reduce the adversary's intelligence collection system by attacking their ability to obtain critical information. This countermeasure includes electromagnetic warfare (EW) against technical collection platforms, offensive cyberspace operations, CI, and physical attacks to degrade and disrupt intelligence capabilities.

OPSEC officers can use more than one measure/countermeasure for each identified vulnerability or a single measure/countermeasure for several identified vulnerabilities. The most desirable OPSEC measure/countermeasure combines the highest possible protection with the least impact on operational resources. Countermeasures should be measurable for performance and effectiveness to allow for analysis and adjustment.

OPSEC measures/countermeasures usually entail some interference with normal operations or impose a cost in time, resources, or personnel. If the cost of implementing measures/countermeasures exceeds the harm the adversary could inflict, the measures/countermeasures may not be appropriate. The decision to employ or not employ a measure(s)/countermeasure(s) requires command-level involvement.

In some situations, the employment of certain OPSEC measures/countermeasures may create additional indicators. For example, camouflaging previously unprotected facilities could indicate preparations for military action. The selection of some countermeasures may require coordination with other components or commands to execute (e.g., jamming intelligence networks or physically destroying them). Conversely, deception and psychological operations plans may preclude applying countermeasures to certain indicators to project a specific message to the adversary.

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

When executing an OPSEC countermeasure, monitor the adversary’s reaction, if possible; determine the countermeasure’s effectiveness; and provide feedback. OPSEC officers use feedback to adjust ongoing activities and for future OPSEC planning. Coordination with associated CI and intelligence organizations ensures OPSEC requirements receive the appropriate attention.

3.7 PERIODIC ASSESSMENT OF EFFECTIVENESS

The OPSEC cycle is a continuous process and should never be considered a one and done requirement. The operational and information environment is constantly evolving, requiring commands to assess their OPSEC posture continuously to maintain essential secrecy.

CHAPTER 4
Assessments

Assessments examine an operation, activity, or organization to determine whether adequate protection from an adversary's intelligence exploitation exists. The assessment helps to identify how and where an organization's critical information is vulnerable to adversarial exploitation.

4.1 TYPES OF ASSESSMENTS

An assessment is an intensive application of the OPSEC cycle or the physical check and validation that an organization can protect its critical information. Assessments are essential to identifying requirements for additional OPSEC measures/countermeasures and making the necessary changes to existing policies and procedures. A thorough assessment validates programs and organizational practices used to protect critical information during day-to-day operations or special activities. There are two types of assessments, internal and external. Command or organic resources generally conduct internal assessments on an annual basis. Teams of external subject matter experts (SMEs) from multiple disciplines perform triennial external assessments emulating the adversary's intelligence processes and capabilities. Figure 4-1 is a comparison of internal and external assessments.

Internal Assessment	External Assessment
Purpose: To examine an organization from the adversary's perspective to determine if current procedures protect critical information, to identify vulnerabilities, and to implement measures/countermeasures.	**Purpose**: To emulate the adversary's intelligence collection capability against an organization to determine if normal operations and functions disclose critical information, to identify vulnerabilities, and to propose measures/countermeasures.
Scale: Small in scale. Focused on evaluating the effectiveness of the organization's OPSEC program.	**Scale:** Large in scale. Focused on analyzing the risk associated with an operation or mission.
Frequency: Annually.	**Frequency:** Triennially or when operations or ISIC dictates.
Resources: Internal, normally manned by members of the organization's OWG.	**Resources:** External (e.g., OPSEC support elements, COMSEC monitors, red teams), with use of a command trusted agent or coordinator. May be covert (i.e., only the commander and trusted agents are aware of the assessment).
Design: Includes planning, execution, and analysis phases and an in-brief and debrief with the commanding officer.	**Design:** Extensive coordination, planning, preparation, execution, and post-execution phases, with a comprehensive final report.

Figure 4-1. Internal and External Assessment Comparison

4.1.1 Difference Between Assessments and Security Inspections

OPSEC assessments are different from security evaluations or inspections. They are not a checklist used to validate administrative compliance or a simple check-in-the-box performed annually.

1. An assessment attempts to produce the adversary's view of an operation or activity. A security inspection seeks to determine if an organization is compliant with the appropriate security directives and regulations.

2. The assessed organization responsible for the operation or activity plans and conducts the assessment. Outside organizations may conduct security inspections without warning.

3. OPSEC assessments do not check the effectiveness of an organization's security programs or its adherence to security directives, although that may be determined during the assessment. Assessment teams seek to determine if any security measures are creating indicators or vulnerabilities.

4. Assessments are not punitive inspections and organizations do not receive a grade or evaluation resulting from the assessment. Assessments do not inspect individuals, but instead assess operations and systems used to accomplish missions.

5. To obtain accurate information, an assessment team creates an environment that promotes positive cooperation and assistance from the assessed organization. Team members question individuals, observe activities, and otherwise gather data during the assessment and make it clear they are not inspectors and their intentions are nonpunitive.

6. The assessed unit's higher headquarters does not receive an assessment report, but the commander or OPSEC assessment team may forward to senior officials lessons learned from the assessment on a nonattribution basis. Senior officials responsible for the operation or activity may decide to further disseminate the lessons learned from the assessment. A best practice is to share lessons learned from the assessment with personnel within the organization to improve the OPSEC posture and mission effectiveness.

4.1.2 Enterprise Protection Risk Management

Enterprise Protection Risk Management (EPRM) is a web-based program hosted on SECRET Internet Protocol Router Network (SIPRNET) that provides commands the ability to conduct security-related assessments across multiple functional areas (security disciplines). Access the OPSEC module within EPRM by first requesting an account via Non-classified Internet Protocol Router Network at: http://eprmhelp.countermeasures.com/.

The Naval Operations Security Support Team (NOST) can assist OPSEC officers with account information and additional resources for EPRM.

4.2 INTERNAL ASSESSMENTS

Conducted annually, the general methodology of an internal assessment applies to all organizations, but specific procedures vary depending on mission focus. An effective internal assessment requires cooperation and participation from all hands since the assessment team—also known as the OWG members—may interview individuals, observe activities, and gather data during the assessment. The OPSEC officer normally leads the assessment and the unit's OWG performs the assessment activities. Small teams of individuals from within an organization, with or without assistance from other SMEs, may also be used. The scope of an OPSEC assessment is usually limited to events and/or activities within the organization. Assessments focus on the organization's routine daily operations or a specific operation, process, or activity. Though missions and functions of different commands vary, there are certain procedural similarities for conducting an assessment. There are three phases of the assessment process—planning, execution, and analysis and reporting.

4.2.1 Planning Phase

Preparations for an assessment begin well in advance. The required lead-time depends on the nature and complexity of the operation or activities assessed (e.g., combat and peacetime operations). OPSEC officers ensure the planning phase includes sufficient time for a thorough review of pertinent processes, documentation, formal and informal coordination, and discussions. The steps of the planning phase include:

1. Determine the Scope. This activity starts the planning phase and limits the assessment to manageable proportions and expectations. Consider geography, time, observation of units, and other practical matters. OPSEC officers identify which command activities, projects, processes, programs, or missions to assess.

2. Brief the Commander. Depending on the command's schedule and battle rhythm, OPSEC officers brief the assessment strategy to the commander. The brief includes the following information:

a. Purpose and Scope. The purpose and scope includes any policy and requirements for the assessment. The purpose statement identifies potential vulnerabilities to command information and identifies mitigations to the vulnerabilities. OPSEC assessments are holistic and most likely cross into other security disciplines (e.g., personnel security, antiterrorism/force protection information security, and physical security).

b. Team Members. List assessment team members by name, department, primary function, and clearance status, if applicable.

c. Schedule. Provide a summary of the plan of action and milestones (POA&M) or schedule of events, highlighting the most significant events (e.g., in-brief, events requiring external support, and brief).

d. Operational Impact. Identify the timeframe and duration of the assessment. Identify planning considerations and operational factors for the chosen assessment period. Identify any impact to the crew (usually no impact) and impact to command operations and missions (usually no impact).

e. Administrative Support Requirements. List outside organizations providing support (e.g., NOST, joint communications security monitoring activity (JCMA), or ISIC). State if internal administrative support is required (e.g., ensuring team members are available from each assigned department or division).

Appendix D provides an example assessment brief.

3. Select Team Members to Augment the Operations Security Working Group (If Required). Select team members for their analytical, observational, and problem-solving skills. OPSEC officers ensure team members represent the functional areas of intelligence, CI, security, communications, logistics, plans, cybersecurity, PA, contracting, acquisition, and administration, if applicable. When appropriate, specialists from other functional areas (e.g., transportation or chemical, biological, radiological, and nuclear) participate. At a minimum, working group and team members:

a. Become familiar with the assessment procedures and techniques, especially when team members do not have previous assessment experience.

b. Understand the assessed operation or activity.

c. Become familiar with the OPLANs, orders, standard operating procedures (SOPs), associated processes, and command policies/directives.

d. Know the command's CIL for the mission. OPSEC officers review and validate critical information throughout the assessment.

e. Become familiar with the command's threat assessment (TA), to include the adversary's primary collection methods, goals, and objectives; intent; and capabilities.

f. Determine the command's current or previous vulnerabilities (e.g., where or how the adversary may obtain critical information).

g. Develop functional outlines for respective areas of interest, knowing the who, what, how, when, where, and why of significant operational events that occur during an assessment. Command profiles are basic guides for this step. Command profiles or functional outlines provide a visual picture of an operation or command.

4. Analyze the Adversary Intelligence Threat. Assessments, primarily conducted from the adversarial perspective, require a comprehensive and current all-source TA. Update the team on any changes to the adversary's intelligence capability and threat information, especially threats most relevant to their command.

5. Review Empirical Studies. Review empirical studies (e.g., COMSEC or CI reports). These reports simulate aspects of the adversary intelligence threat and support vulnerability findings.

4.2.2 Execution Phase

The primary actions conducted during the execution phase are physical collection of information and data through observation of activities, personnel interviews, verification of command personnel following policy, and collection of empirical data through open-source research (OSR) and COMSEC monitoring reports.

1. Data Collection. Assessment team members must be alert to differences between what they read, what they assume to be the situation, what they learn from the command briefing, and what they observe. Expect conflicting data, team members adjudicate this data during the assessment period. A best practice is to assign a team member to lead an assessment area or function throughout the duration of the assessment. This provides the OPSEC officer the opportunity to monitor the assessment holistically, keep the assessment on track per the POA&M, and collect data from each team member at the end of each day.

a. Open-source Research. Conduct OSR to ensure the command is not publishing or posting critical information in publicly available information (PAI) environments. This includes reviewing the command's public facing website, official social media pages, and a rudimentary search of what command members are posting online. The review includes information contained in contracts, job announcements, Navy family ombudsman or readiness group pages, and any other information published to the public.

b. Administrative Review. Conduct administrative reviews to determine if command members are following command policy. For example, if it is the command's policy to shred all printed paper products, then the assessment team should not find printed paper products in the trash or dumpsters. OPSEC and security policies can include the badging in/out process, quarterdeck procedures, visitor check procedures, recycling versus shredding, burn bag procedures, email encryption, declaration of phone-up/phone-down practice, logging visitors in/out of classified spaces, and portable electronic device policy. The assessment team must know the policies and procedures to spot or observe a potential vulnerability. Figure D-10 in Appendix D provides an administrative policy checklist.

c. Office, Compartment, or Space Walk-through. Assessment team members conduct a walk-through of the organization's offices, compartments, and spaces to identify potential OPSEC vulnerabilities and policy discrepancies. Team members check for items, such as phone stickers (DD 2056, Telephone Monitoring Notification Decal), inoperable shredders, computer screens facing windows, safes requiring repair or safes improperly unlocked, portable electronic devices in secure areas, classified or sensitive information requiring destruction (overflowing burn bags), passwords or safe combinations written down, etc. Team members document policy discrepancies and report security violations identified during the walk-through.

d. Stand Off Observations. Observation from a distance can reveal a lot about an organization and its personnel. If the adversary wants to gain access to an installation, they could conduct some level of surveillance or stand off observations to look for a weakness or vulnerability in procedures. For example, the best opportunity to access a facility may be during heavy-traffic (vehicle or foot) times, when security does their best to prevent jams or backups. Photography of security badges when not secured or openly worn outside, makes replication easier. Observation of when doors are open or secured during the day, or whether or not piggybacking occurs, can lead to easy access. The adversary may observe if security cameras are present and functioning, and when watch standers turnover. Figure D-11 in Appendix D provides an observation checklist.

e. Command Member Interviews/Questionnaires. Talking to or interviewing personnel about OPSEC can best define the command's OPSEC culture. The Navy uses interviews (knowledge checks), to determine skill level and qualification status, and questionnaires (surveys), to determine command climate. The better the OPSEC culture, the less likely vulnerabilities will exist. Interviews should be nonintrusive to command operations and personnel, short and concise, and tailored to the command's mission, operation, or basic need for specific information. The percentage of interviews depends on the organization, but a best practice is roughly 25–30 percent of the organization. Figure D-12 in Appendix D provides sample interview questions.

f. Dumpster Dives. We often take for granted or just turn a blind eye when it comes to determining what information we are potentially discarding. In years past, the messenger of the watch aboard every ship inspected trash prior to crossing the quarterdeck at the end of the day. Most shore organizations have an all-shred policy; however, commands seldom verify members are following the policy. Because recycled papered is typically not reviewed for critical information, the recycling of whole paper has created an additional vulnerability. A best practice is for a member of the security department or OWG to check individual space trashcans at the end of the day for printed materials while conducting office, compartment, or space walk-throughs. Commands can easily mitigate the vulnerability of placing discarded classified and critical information in the trash by instituting and verifying an all-shred policy. Commands can validate policies are being followed by periodically reviewing the trash during internal assessments or spot checks. Figure D-13 in Appendix D provides a trash inspection checklist.

2. Findings. Report to the chain of command, for immediate mitigation or corrective action, any finding during the assessment considered to have a serious impact to the command's mission or discovery of a security violation.

a. As previously stated, a best practice is to assign team members to lead an assessment area or function (e.g., OSR, observations, interviews, administrative review). At the end of each day, or earlier, the team leads report all findings to the OPSEC officer for consolidation and preparation of the assessment brief to the commander. Conduct end-of-day hot wash for team members to share, discuss, and adjudicate any findings.

b. A picture tells 1,000 words. Take photographs of findings, if possible, and include them in the final brief. Photograph discovered critical information, personally identifiable information (PII), or other printed material to highlight the vulnerability, while also protecting the PII and potential violator. Remember, internal assessments are nonattributional.

4.2.3 Analysis and Reporting Phase

OPSEC officers and assessment teams compile, correlate, and analyze the collected data. The team identifies any potential vulnerabilities, poor OPSEC practices, and other security violations, and determines the command's ability to protect critical information. The team recommends a measure/countermeasure for each identified vulnerability. The OPSEC officer submits a final report or debriefs the commanding officer on findings and measures/countermeasures recommendations upon completion of this phase. Appendix D provides an example debrief template.

1. The final report or debrief is usually in PowerPoint format, but it is up to the command to decide which format or how to brief the commander. The report includes the command's CII, the adversary's collection capabilities, vulnerabilities identified during the assessment, and recommended measures/countermeasures. Although some vulnerabilities may be impossible to eliminate or mitigate, OPSEC officers include them in the report to enable the commander to fully assess the command, operation, or activity.

2. OPSEC officers track all findings until resolved. For example, if the vulnerability is personnel piggybacking or improperly badging, the proposed measure is to post a watch during high-traffic times to monitor and inform personnel of proper procedures. This requires creating a schedule of who, when, and where the watch takes place. Conditioning command members to properly badge in and out of the command should only take a few days. Another example is if printed material is discovered in the dumpster, the proposed measure is to conduct a daily trash check. Upon successful mitigation of the vulnerability, consider reducing trash checks to once a week and then monthly. These are examples of how OPSEC officers can combat a vulnerability.

3. Assessments are required annually; however, maintain assessment findings for a minimum of three years to establish trends. Measures of performance (MOPs) and measures of effectiveness (MOEs) can also be established and even reported up the chain of command for best practices.

4.3 EXTERNAL ASSESSMENTS

An external assessment is required triennially and conducted by a team of SMEs from multiple disciplines, external from the command, to simulate adversary intelligence processes. External resources (the assessment team) focus on the organization's ability to protect critical information from adversary intelligence exploitation during planning, preparation, execution, and post-execution phases of an operation or activity. Despite the triennial requirement from the DOD, the Navy is not equipped or resourced to meet this requirement. As a result, higher headquarters at echelon III or above direct the execution of external assessments. Internal and external assessments have many common functions. Additional external assessment functions may include:

1. Communications Security Monitoring. JCMA at NSA provides COMSEC monitoring of Navy networks on a not-to-interfere basis with real-world operations. JCMA primarily supports the combatant commander (CCDR) on a near-continuous basis, which means ships operating in the United States Central Command, United States European Command, United States Indo-Pacific Command, and United States Africa Command areas of responsibility (AORs) are subject to monitoring. JCMA may provide monitoring support during Carrier Strike Group (CSG) FOUR and FIFTEEN's composite training unit exercise, on a not-to-interfere basis. Navy shore commands requesting JCMA support are not likely to get approval. For additional information, refer to NTISSD 600, Communications Security Monitoring; and OPNAVINST 2201.3C, Communications Security Monitoring of Navy Telecommunications and Information Technology Systems; or contact the NOST.

2. Elicitation. Elicitation is often synonymous with HUMINT, which is essentially collecting information about an organization or operation through human interaction, often trusting the individual with whom you are sharing information. Most of the Services' investigative capabilities (e.g., NCIS, United States Army Criminal Investigative Division, and United States Air Force Office of Special Investigation) conduct elicitation activities in support of criminal investigations. Elicitation support is difficult to request for OPSEC assessment purposes due to resourcing and other higher priority tasking. It is prudent to review the HUMINT threat for your area well in advance of an assessment. Find a current list of threat briefings on NCIS' SIPRNET homepage at: https://www.ncis.navy.smil.mil/.

3. Network and Computer Systems Assessments. The Navy has a network assessment capability, also known as the Navy red team (NRT), located at Navy Cyber Defense Operations Command in Suffolk, Virginia. The NRT supports CCDR exercises and units during the optimized fleet response plan (OFRP) to test network security and network hygiene. The NRT notoriously sends phishing emails and attachments to command members to test their knowledge or to access a command's network.

4. Close Access Team (CAT). Physical access equals network access. When the NRT is unable to gain access to a network remotely via phishing or other technical means, they may turn to their CAT personnel who attempt to gain access via physical means. This includes elicitation techniques, replication of security badges, posing as friendly contractors, or solicitation of specific information—all in an attempt to gain physical access to the network. The CAT seldom fails to gain network access. NRT and CAT assets are extremely limited.

5. Radio Frequency (RF), Electronic, and Wi-Fi Monitoring. Request or perform internally, if equipment is available, RF, electronic, and Wi-Fi monitoring. For example, if an organization prohibits wireless devices, purchase a wireless hand-held detection device to monitor for wireless devices in prohibited spaces.

6. Open-source Research. Similar to reviewing the PAI environment during an internal assessment, organizations can request specialized OSR services from external organizations that specialized in using artificial intelligence and data mining programs to conduct OSR. The United States Marine Corps OPSEC support team has grown their own OSR capability, but faces resource constraints. Other specialized or contracted organizations may come at a cost. Contact the NOST for additional information about organizations that specialize in OSR and data mining.

4.4 OPTIMIZED FLEET RESPONSE PLAN REQUIREMENTS

Every unit in the training cycle and scheduled for deployment, whether as part of a strike group or individual deploying unit, is responsible to establish and maintain a proactive OPSEC program. This section discusses the roles and responsibilities of Naval Information Warfare Training Group (NIWTG) located in Norfolk, Virginia, and San Diego, California.

Units prepare for deployment by undergoing a required assessment of their OPSEC program assessed by NIWTG during the OFRP. When included in the OFRP, the commander and information warfare commander (IWC) get a better understanding of their unit's OPSEC posture. During the OFRP, NIWTG:

1. Provides OPSEC officers and coordinators an opportunity to attend the Navy OPSEC course (J-2G-0966). OPSEC courses occur regularly on each coast and in fleet-concentrated areas.

2. Schedules and conducts an assist visit with the ship's OPSEC officer. The initial visit determines the status of the ship's OPSEC program, and provides OPSEC officers with the necessary tools to establish or improve their program. This includes training on conducting internal assessments.

3. Provides feedback and recommendations for improvement on the ship's overall OPSEC program and posture following the completion of the internal assessment. Validation and review typically occurs within 30 to 45 days after the initial assist visit.

4. Provides written reports to OPSEC officers addressing the ship's overall OPSEC posture.

INTENTIONALLY BLANK

CHAPTER 5

Operations Security in Messages

5.1 SCOPE

OPSEC reduces the risk of compromising critical information in a variety of messages and emails ranging from operations and protocol, to medical support requests. Implementing OPSEC denies the adversary knowledge of friendly force practices, capabilities, and planning details. This chapter provides guidance on writing OPSEC messages during potentially high-visibility situations.

5.2 SITUATIONAL MESSAGES

Conducting naval operations is dangerous and extremely unpredictable. Even during routine operations, a simple error in judgement can result in a catastrophic event and even loss of life. Most recently, the Navy experienced at-sea collisions, unforeseen fires and flooding, crew infections/pandemics, and aircraft crashes and collisions. These examples were unexpected situations that occurred with little to no warning.

When an event occurs, measures/countermeasures are employed immediately to protect the force and control critical information. In today's IE, the instantaneous uploading and sharing of information in the PAI environment makes controlling the critical information extremely difficult. Afloat units employ River City as a means to control the critical information following an event. River City is an information management tool to maintain OPSEC or limit information release after an event (e.g., a mishap or man overboard). Releasing an official naval message as a reminder to practice OPSEC is a best practice, especially when an event may continue for longer periods. The force and other organizations involved in the event should be reminded to practice proper OPSEC procedures. Reporting up and down the chain of command, sharing information with those who have a need to know, and informing the public at the same time can be a balancing act. This section covers drafting an OPSEC message as a reminder to protect critical information during an unforeseen event.

The first portion of a situational message is the header, which includes the originator, list of addressees, classification, subject line, and OPSEC references. The physical location of the event or AOR where the event occurred, dictates much of the header information, although there are no boundaries in today's IE. Figure 5-1 depicts an example header of a situational message.

```
P XXXXXXZ MMM YY
FM (ORIGINATOR)
TO (LIST OF RECIPIENTS)
INFO (INCLUDE ANY INFORMATION ADDRESSEES)
CLASSIFICATION
MSGID/
SUBJ/OPERATIONS SECURITY IN SUPPORT OF (EVENT/SITUATION)//
REF/A/DOC/SECNAVINST 3070.2A/09 MAY 19//
REF/B/DOC/SECNAVINST 5720.44/14 OCT 14//
REF/C/DOC/(ANY REFERENCES REGARDING SITUATION)//
NARR/ REF A IS SECNAVINST 3070.2A, OPERATIONS SECURITY. REF B IS
SECNAVINST 5720.44C WITH CHANGE 2, DON PUBLIC AFFAIRS POLICY AND
REGULATIONS. REF C IS (DESCRIBE THE EVENT/SITUATION OR ANY OTHER
REFERENCE TO THE EVENT/SITUATION).
```

Figure 5-1. Header Example

Like most naval messages, it is mandatory to state the purpose of the message. In Figure 5-2, the purpose of this situational message is to inform all concerned of the importance to protect critical information or practice OPSEC following or during an event. For example, in April 2009, during the rescue of Captain Richard Phillips of *Maersk Alabama* from Somali pirates, a Sailor's blog divulged specific details of the event. The information quickly made national headlines and could have aided the pirates or tribal leaders directly involved.

```
1. RMKS// (X) PURPOSE. TO CLEARLY ARTICULATE OPERATIONS SECURITY
(OPSEC) DIRECTION AND EXPECTATIONS TO (LIST FLEET OR COMMANDS
DIRECTLY INVOLVED) FORCES AND PERSONNEL DURING THE (EVENT/SITUATION)
IN ACCORDANCE WITH DEPARTMENT OF THE NAVY OPSEC POLICIES PROVIDED IN
REFS A AND B.
```

Figure 5-2. Purpose Example

Regardless of the AOR or fleet the event takes place in, there is most likely an OPORD, operational tasking, or fleet communication plan that provides specific fleet guidance on controlling information or provides specific OPSEC guidance. It is important to review and follow fleet OPSEC guidance prior to joining a particular AOR. The background section states the AOR/fleet OPSEC requirement and how it relates to the event. Figure 5-3 is an example background section of a situational message.

```
2. (X) BACKGROUND.

2.A. (X) IN LINE WITH THE NAVY (APPROPRIATE NAVY GUIDANCE GIVEN
CURRENT EVENT/SITUATION), (FLEET OR COMMAND) FORCES WILL CONTINUE
MILITARY OPERATIONS. REGIONAL ADVERSARIES, SUCH AS (NAME YOUR
COUNTRIES) ALSO CONTINUE MILITARY OPERATIONS IN THE MARITIME
THEATER.//

2.B. (X) REGARDLESS OF THE PRESENT CIRCUMSTANCES, OPSEC SHALL BE
MAINTAINED. ANY INFORMATION THAT RELATES TO THE (FLEET OR COMMANDS)
OPERATIONAL ASPECTS OF PRESENCE, CAPABILITY, STRENGTH, INTENT,
READINESS, TIMING, LOCATION, AND METHOD OR CRITICAL INFORMATION WILL
BE PROTECTED, REGARDLESS OF THE METHOD OF COMMUNICATION. OPSEC
EXISTS TO PROTECT OUR ESSENTIAL SECRETS AND UNCLASSIFIED CRITICAL
INFORMATION THAT DIRECTLY RELATE TO OUR OPERATIONAL ASPECTS.
```

Figure 5-3. Background Example

Provide the current threat and/or adversary information in the next paragraph of the situational message. The information acquired from intelligence sources may result in classifying the message, which limits the distribution guidance. To ensure widest dissemination make every effort to keep the message unclassified or controlled unclassified information (CUI). The bottom line, the adversary may be interested, observe, and collect friendly force actions and reactions given the event, especially friendly force TTP. Practicing OPSEC and protecting critical information derived from operational aspects is paramount, so be specific and concise. See Appendix A, step 2, for information on how to identify the operational aspects that apply to the situation. For example, in a ship's collision, capability and readiness are the operational aspects that apply. Protect any information related to capability and readiness from adversary exploitation. Figure 5-4 is an example threat section of a situational message.

```
3. (X) THREAT.

3.A. (X) THE (EVENT/SITUATION) PROVIDES A UNIQUE OPPORTUNITY FOR
REGIONAL ADVERSARIES TO GAIN VALUABLE KNOWLEDGE REGARDING THE (LIST
OPERATIONAL ASPECT(S) THAT PERTAIN) OF THE U.S. NAVY AND MILITARY.
IN PARTICULAR, ADVERSARIES WILL SEEK TO GAIN AN UNDERSTANDING OF OUR
OPERATIONAL PRIORITIES, CRISIS MANAGEMENT PROCESSES, CRISIS COMMAND
AND CONTROL (C2), AND FLEET REACTION/MOVEMENTS.

3.B. (X) REGIONAL ADVERSARIES WILL ALSO BE KEENLY OBSERVING THE
(LIST OPERATIONAL ASPECT(S) THAT PERTAIN) STATUS OF U.S. NAVY AND
MILITARY FORCES. A PERCEIVED DECLINE IN OUR ABILITY TO COUNTER
FOREIGN ACTS OF AGGRESSION MAY PRESENT ADVERSARY DECISION MAKERS
WITH A BATTLEFIELD ADVANTAGE, WHERE THEY MAY CAPITALIZE UPON OUR
PERCEIVED VULNERABLE STATE TO ACT AGGRESSIVELY OR ACCORDINGLY IN
ORDER TO ACHIEVE THEIR STRATEGIC AND OPERATIONAL OBJECTIVES.
```

Figure 5-4. Threat Example

Any unpredicted event may inherently disrupt or have some level of impact on friendly force operations. It is important to mention the immediate impact and disruption to operations in the situational message. Doing so provides all concerned parties with vetted information to control future messaging. At a minimum, address the disruption of routine operations and any expected press/media attention. For example, continuing with the ship collision scenario, the impact may be a return to homeport change, an unscheduled port visit for damage assessment, damage control procedures, and communication outages or conditions (River City). Figure 5-5 is an example impact section of a situational message.

```
4. (X) IMPACT. (LIST THE IMPACT THE EVENT/SITUATION HAS CAUSED
(DISRUPTION OF ROUTINES, PRESS/MEDIA ATTENTION, TELEWORKING)).
```

Figure 5-5. Impact Example

The impact section is the most important paragraph of the situational message because it contains OPSEC direction and guidance to all concerned organizations and parties involved. Provide specific guidance, orders, and any ramifications of violating the orders or guidance. Refer to any fleet or AOR guidance, if applicable. This is an excellent time to remind Sailors of their duties and responsibilities to perform and act professionally, especially during adverse situations. All too often, people are quick to share, chat, upload photos and videos, and post information without completely understanding the potential adverse effects of the message. For example, it is not appropriate to post photos of damage or information about a missing or injured shipmate. Uploaded photos may reveal ship's readiness and capabilities (operational aspects) to the adversary and posting about the status of another shipmate does not align with good order and discipline. Disclosure of critical information about the ship or personal information about a shipmate requires proper vetting and authorization by the commanding officer. Figure 5-6 is an example OPSEC direction section of a situational message.

The countermeasures in Figure 5-6 are not all-inclusive. Ultimately, common sense prevails when drafting messages or sending email or chat sessions that contain potentially critical information. If transmitting critical information is necessary via nonsecure means, make every effort to minimize the amount of information at risk.

```
5. (X) OPSEC DIRECTION FOR ALL HANDS. PER (FLEET OR COMMAND),
INFORMATION REGARDING (EVENT/SITUATION) IS CONSIDERED (CLASSIFIED
(TS/S/C)) OR CRITICAL UNCLASSIFIED INFORMATION. ALL HANDS SHALL
REFRAIN FROM DISCUSSING THE (EVENT/SITUATION AND ASSOCIATED ACTIONS)
ON UNCLASSIFIED NETWORKS, PHONE LINES, LETTERS, OR ANY OTHER
UNSECURE COMMUNICATIONS CHANNELS.

5.A. (X) THIS OPSEC POLICY DOES NOT INFRINGE UPON THE FIRST
AMENDMENT RIGHTS GRANTED TO EVERY SAILOR AS A PRIVATE CITIZEN TO
FREELY EXPRESS THEMSELVES ONLINE IN AN UNOFFICIAL CAPACITY.

5.A.1. (X) HOWEVER, WHEN ONLINE, WE AS SAILORS MUST RECOGNIZE THAT
WE MAY BE PERCEIVED AS A SPOKESPERSON FOR THE NAVY SIMPLY BECAUSE WE
WEAR THE UNIFORM. WE MUST REMEMBER OUR RESPONSIBILITY TO CONDUCT
OURSELVES PROFESSIONALLY AND ENSURE THAT WE DO NOT DISCLOSE
SENSITIVE INFORMATION RELATED TO THE PRIVACY OF INDIVIDUALS,
READINESS OF THE FLEET, OR OPSEC.

5.A.2 (X) THE NAVY SOCIAL MEDIA HANDBOOK (REF X) PROVIDES ADDITIONAL
GUIDANCE REGARDING APPROPRIATE ONLINE SOCIAL MEDIA CONDUCT AND
OPSEC. ANY VIOLATION OF APPROPRIATE ONLINE SOCIAL MEDIA CONDUCT
AND/OR OPSEC MAY RESULT IN ADMINISTRATIVE OR DISCIPLINARY ACTION IN
ACCORDANCE WITH THE UNIFORM CODE OF MILITARY JUSTICE. THE HANDBOOK
AND OPSEC GUIDANCE CAN BE FOUND ON LINKS FROM THE NAVY HOME PAGE AT
WWW.NAVY.MIL OR WWW.NAVIFOR.USFF.NAVY.MIL/OPSEC.

5.A.3 (X) IAW REFS A AND B, BE MINDFUL OF INFORMATION ONLINE THAT
WAS NOT RELEASED THROUGH OFFICIAL CHANNELS. REFRAIN FROM ENGAGING IN
SPECULATIVE RUMORS OR UNOFFICIALLY LEAKED INFORMATION.

5.A.4 (X) SAILORS MAINTAIN THE RIGHT TO DISCUSS THEIR PRIVATE STATUS
WITH WHOMEVER THEY CHOOSE. IN THIS TIME OF (EVENT/SITUATION),
CONTINUED COMMUNICATIONS WITH FAMILY MEMBERS IS ENCOURAGED AS LONG
AS THEY DO NOT DISCUSS INFORMATION WHICH DIRECTLY RELATES TO OUR
OPERATIONAL ASPECTS STATED ABOVE. SAILORS WILL REMAIN COGNIZANT OF
DOWNSTREAM EFFECTS OF PERSONAL INFORMATION THEY SHARE, ESPECIALLY
HOW THIS INFORMATION COULD BE PERCEIVED BY THE PUBLIC WITH REFERENCE
TO FLEET OR COMMAND READINESS.

5.A.5. (X) IF DIRECTLY QUERIED BY A MEMBER OF THE MEDIA, SAILORS
MUST CONSULT WITH THEIR LOCAL UNIT OR COMMAND PUBLIC AFFAIRS OFFICE
FOR GUIDANCE ON MEDIA INTERACTIONS.

5.B. (X) COMPLIANCE BY ALL PERSONNEL IS MANDATORY. WE MUST NOT
PROVIDE ANY INDICATION TO ANY POTENTIAL ADVERSARIES THAT THE U.S.
NAVY IS OPERATING IN A DEGRADED STATE OR DOES NOT CURRENTLY POSSESS
THE CAPABILITY TO PROTECT OURSELVES, OUR ALLIES, OR OUR PARTNERS.
KEEPING THE ADVANTAGE WHILE DENYING THE ADVERSARY CRITICAL
INFORMATION, INDICATORS, AND ESSENTIAL SECRETS IS HOW WE PROTECT OUR
FLEET.//
```

Figure 5-6. Operations Security Directions Example

Disseminate the OPSEC situational message to all parties/personnel directly involved with the event. Include a coordination paragraph to provide staffs, commanders, and/or OPSEC officers with direction on actions to take and reporting guidance. List point(s) of contact details. Figure 5-7 is an example coordination section of a situational message.

Note

Reporting guidance may not be necessary for situations/events that involve a single unit. However, an event/situation affecting the fleet or an AOR (i.e., pandemic) should contain reporting guidance.

```
6. (X) COORDINATION. ALL COMMANDERS AND/OR OPSEC OFFICERS SHALL
DISSEMINATE THIS OPSEC POLICY TO STAFFS AND UNITS UNDER THEIR
COMMAND VIA EMAIL AND SHALL BE RESPONSIBLE FOR 100 PERCENT
ACKNOWLEDGEMENT BY ALL HANDS. REPORT ACKNOWLEDGEMENT TO (CTF OR ISIC
OVERSEEING THE SITUATION).

7. (X) POINTS OF CONTACT

7.A. (X) NAME, TITLE, AND PHONE NUMBER

7.B. (X) NAVAL OPSEC SUPPORT TEAM, NAVAL INFORMATION FORCES,
OPSEC(AT)NAVY.(SMIL).MIL, 757-203-3656. (DSN: 668)
```

Figure 5-7. Coordination Example

INTENTIONALLY BLANK

CHAPTER 6
Operations Security Planning

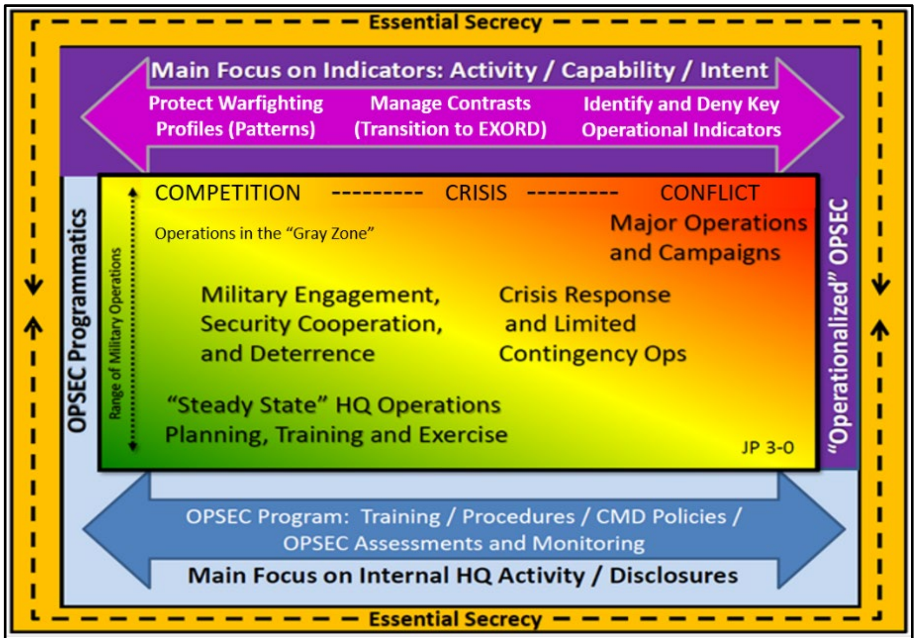
6.1 PURPOSE

This chapter provides detailed guidance to OPSEC planners on naval staffs at the operational level of warfare (OLW). It combines the concepts discussed in this publication into a systematic planning process for use by OPSEC planners. This chapter presents new concepts derived from the DOPC, such as friendly activity mapping, the creation of a preliminary critical information and indicator list (CIIL), OPSEC tasks, and effects-based OPSEC measures and countermeasures coordinated through OPSEC event planning.

OPSEC planners can typically utilize the OPSEC cycle and mission planning concepts within the plan, brief, execute, debrief (PBED) process for conducting OPSEC planning at the tactical level of warfare. Refer to NWP 5-01, Navy Planning, for more information on the PBED process.

6.2 THE OPERATIONS SECURITY PROGRAM AND OPERATIONS SECURITY PLANNING

In addition to maintaining an OPSEC program, focused operational OPSEC planning is necessary to reduce risk to mission and forces in a dynamic OE. While a well-managed command OPSEC program sets the baseline for day-to-day activities by protecting critical information, a command's OPSEC program and CIL are usually insufficient to satisfy planning for specific operations or future OPLANs. To integrate OPSEC into operational planning efforts and specific operations, the Navy planning process (NPP) must include OPSEC planning. OPSEC planning seeks to achieve and maintain essential secrecy by denying the adversary knowledge of friendly force operational aspects through the management and control of operational profiles, the reduction or hiding of contrasts, and the reduction or elimination of exposures of friendly force operational indicators. Both the OPSEC program and execution of operational plans must work together to achieve and maintain essential secrecy. Figure 6-1 depicts the relationship between the OPSEC program and operationalized OPSEC.


Essential Secrecy
Main Focus on Indicators: Activity / Capability / Intent
Protect Warfighting Profiles (Patterns)
Manage Contrasts (Transition to EXORD)
Identify and Deny Key Operational Indicators
COMPETITION --------- CRISIS --------- CONFLICT
Operations in the "Gray Zone"
Major Operations and Campaigns
Range of Military Operations
Military Engagement, Security Cooperation, and Deterrence
Crisis Response and Limited Contingency Ops
"Steady State" HQ Operations Planning, Training and Exercise
JP 3-0
OPSEC Programmatics
"Operationalized" OPSEC
OPSEC Program: Training / Procedures / CMD Policies / OPSEC Assessments and Monitoring
Main Focus on Internal HQ Activity / Disclosures
Essential Secrecy

Legend:

CMD	command	EXORD	execute order	HQ	headquarters

Figure 6-1. Operations Security Program and Operationalized Operations Security

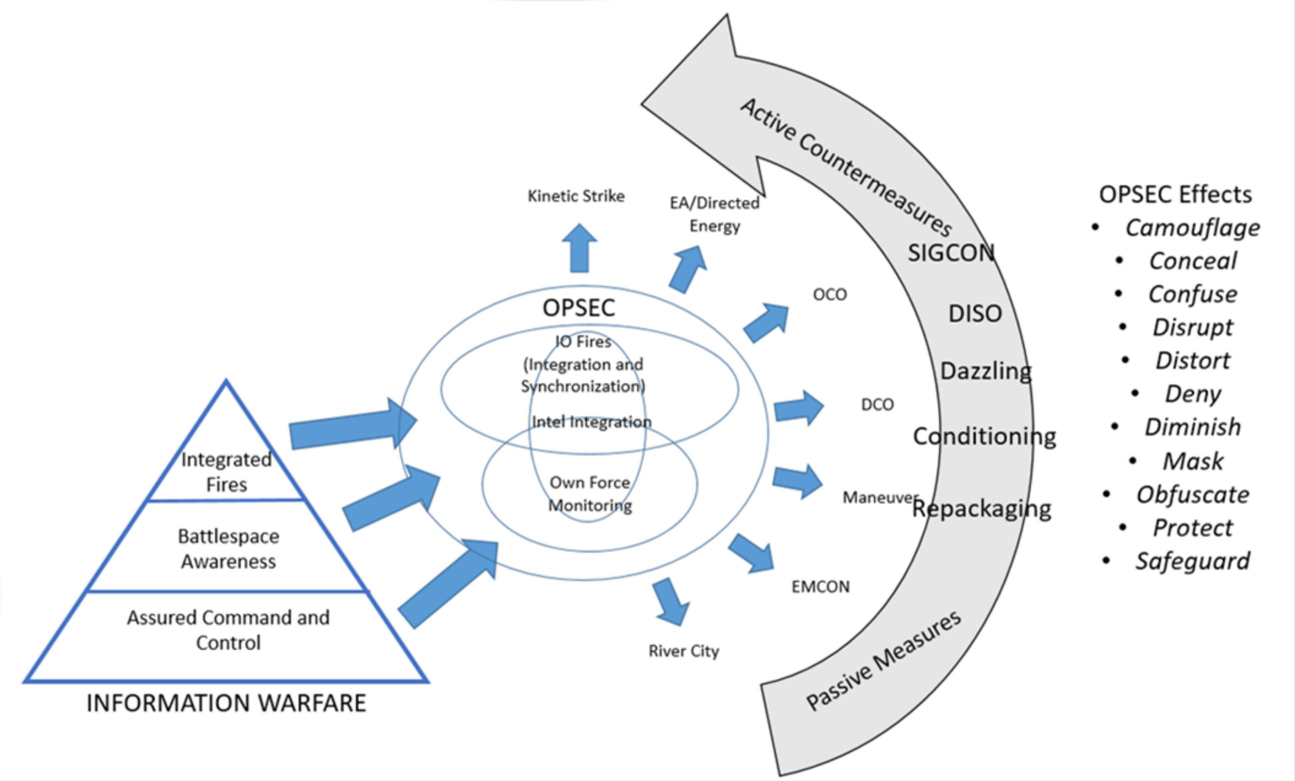
6.3 INFORMATION OPERATIONS AND INFORMATION WARFARE INTEGRATION

The core pillars of information warfare (IW) include assured command and control, battlespace awareness, and integrated fires. By integrating and synchronizing intelligence functions, battlefield networks, and kinetic and nonkinetic fires, the naval commander can achieve information superiority over the adversary. Information superiority is the operational advantage derived from the ability to collect, process, and disseminate an uninterrupted flow of information while exploiting or denying the adversary's ability to do the same.

Naval commanders use IRCs to conduct IW to achieve kinetic and nonkinetic effects in the IE. As one of the IRCs, OPSEC is a vital aspect in achieving information superiority and maintaining essential secrecy by disrupting the adversary's decision-making cycle.

Navy staff information operations (N39)/fleet IW cells, at the high OLW (combined force maritime component commander/fleet maritime operation center), integrate and synchronize OPSEC into operational plans. This provides the commander the ability to deny key friendly operational aspects to the adversary and allows friendly forces to gain the surprise, protect operational concepts and methods, mitigate operational vulnerabilities, and achieve desired effects in the IE at decisive points in space and time.

At the low OLW, task force commanders execute guidance from integrated IW plans and use OPSEC plans to manage and control the tactical situation, achieve tactical surprise, create operational unpredictability, and protect critical capabilities and intentions. Individual units at the tactical level of warfare execute OPSEC measures and countermeasures to create a comprehensive and coherent operational profile within the IE, under the guidance of the task force commander. Figure 6-2 depicts the integration of operationalized OPSEC with IW.



Legend:

DCO	defensive cyberspace operations	EMCOM	emission control	OCO	offensive cyberspace operations
EA	electronic attack	IO	information operations	SIGCON	signature control

Figure 6-2. Operationalized Operations Security Integration with Information Warfare

6.4 SPECIAL RELATIONSHIP WITH MILITARY DECEPTION

OPSEC and MILDEC share a special relationship—both are capabilities that utilize the IE to achieve specific effects. OPSEC seeks to protect CII by safeguarding, obfuscating, or concealing information from adversary intelligence entities. MILDEC projects false information to create alternate profiles to the adversary decision maker and attempts to influence the decision maker into COAs advantageous to friendly forces. Organizations cannot execute MILDEC without an effective OPSEC plan. OPSEC and MILDEC planners work hand in hand to create a cohesive narrative in the IE.

DISO is a military deception activity that protects friendly operations against adversary collection by creating false indicators to make friendly force operational aspects harder to interpret by the adversary intelligence entity. Only conduct DISO under proper authorization, when traditional OPSEC measures/countermeasures are insufficient to mitigate OPSEC vulnerabilities. Figure 6-3 depicts the relationship between OPSEC and MILDEC.

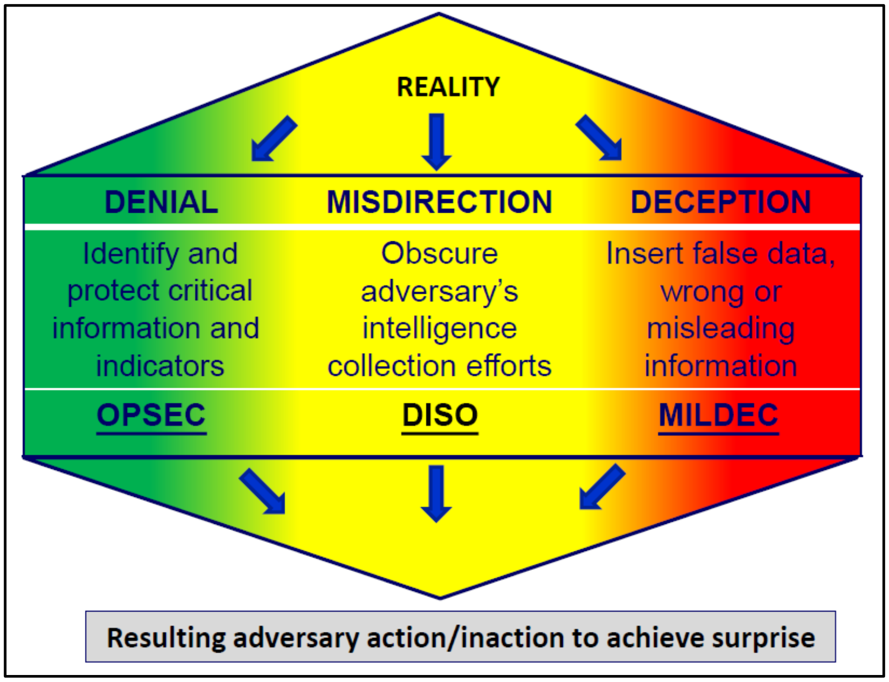

REALITY
DENIAL
MISDIRECTION
DECEPTION
Identify and protect critical information and indicators
Obscure adversary's intelligence collection efforts
Insert false data, wrong or misleading information
OPSEC
DISO
MILDEC
Resulting adversary action/inaction to achieve surprise

Figure 6-3. Operations Security and Military Deception Relationship

6.5 OPERATIONS SECURITY IN THE NAVY PLANNING PROCESS

OPSEC planners integrate OPSEC into each step of the NPP and coordinate closely with other planners, specifically those who coordinate and task other IRCs. As a best practice, OPSEC planners integrate into the IW cell to facilitate integration across the IRCs. OPSEC planners are recommended to attend the Joint Information Operations Planners' Course or DOPC. OPSEC inputs and deliverables to the NPP occur during COA development, COA wargaming and analysis, and COA comparison and decision phases of planning. This makes problem framing or mission analysis essential to the planning process and is where OPSEC planners focus their planning efforts. OPSEC planners develop planning estimates that serve as vital inputs to the planning team and helps the commander make fully informed decisions while considering OPSEC implications of each COA. Figure 6-4 depicts the integration of OPSEC into the NPP.

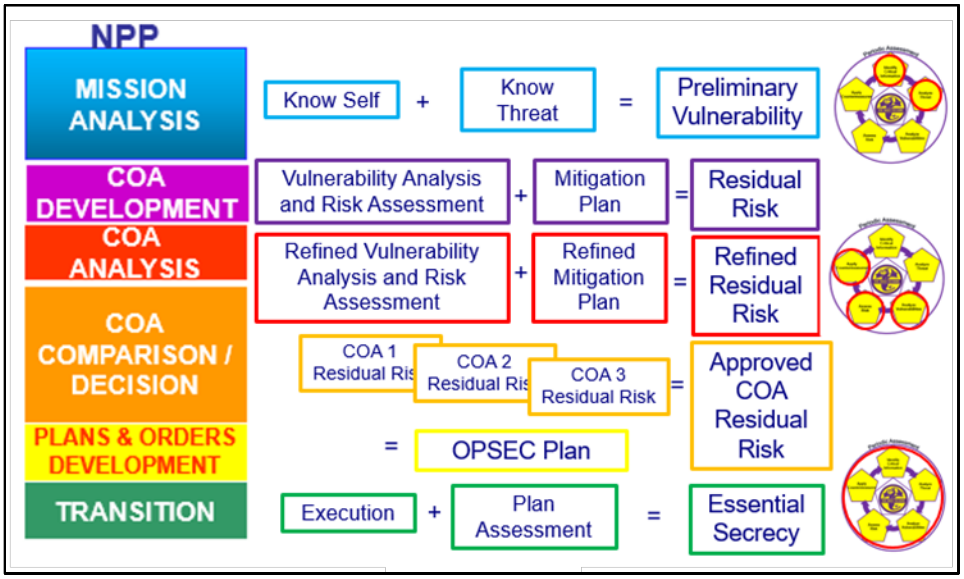

NPP
MISSION ANALYSIS
COA DEVELOPMENT
COA ANALYSIS
COA COMPARISON / DECISION
PLANS & ORDERS DEVELOPMENT
TRANSITION
Know Self + Know Threat = Preliminary Vulnerability
Vulnerability Analysis and Risk Assessment + Mitigation Plan = Residual Risk
Refined Vulnerability Analysis and Risk Assessment + Refined Mitigation Plan = Refined Residual Risk
COA 1 Residual Ris
COA 2 Residual Ris
COA 3 Residual Risk = Approved COA Residual Risk
= OPSEC Plan
Execution + Plan Assessment = Essential Secrecy

Figure 6-4. Operations Security Integration into the Navy Planning Process

6.6 OPERATIONS SECURITY MISSION ANALYSIS AND STAFF ESTIMATE

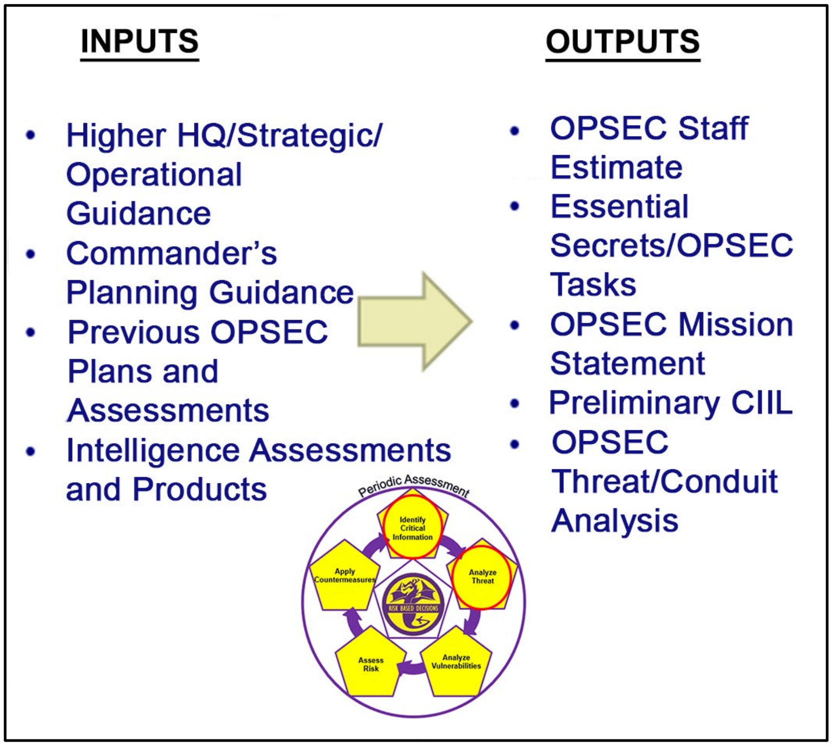
OPSEC planners identify critical information and conduct threat analysis during the mission analysis step of the NPP. They work from guidance provided by higher headquarters to determine what information requires OPSEC protection, examine friendly operations to identify operational indicators, and conduct threat analysis to develop a staff estimate to provide to the IW cell, planning working groups, and commander, if necessary.

An OPSEC staff estimate identifies what critical information requires protection through OPSEC tasks, defines the OPSEC mission statement, and includes a preliminary CIIL and OPSEC threat analysis. OPSEC planners work with intelligence counterparts to analyze potential adversaries, conduct conduit analysis of adversary intelligence, surveillance, reconnaissance, and targeting (ISRT) systems, and develop profiles of the IE. Completing the first two steps in the OPSEC cycle allows an OPSEC planner to develop a written OPSEC staff estimate that outlines the OPSEC requirements in COA development and the overall OPSEC plan. Use information derived from the staff estimate to inform other products (e.g., reveal and conceal guidance to the force). Figures 6-5 depicts the inputs to the mission analysis step of the NPP and the OPSEC outputs.

6.6.1 Operational Aspects (Essential Secrets), Operations Security Tasks and Mission Statements

Recognizing that if the adversary understands specific friendly force operational aspects, they can disrupt friendly force operations, the staff estimate answers the question of what operational aspects to protect to accomplish the mission. These operational aspects are the essential secrets of friendly operations. The operational aspects (see 3.1) are presence, capability, strength, intent, readiness, timing, location, and method. It is not necessary to protect all operational aspects at all times. For example, a naval force conducting a show of force, may want to project to the adversary the aspects of presence, strength, and capability, but protect other aspects, such as readiness or intent. This allows the OPSEC planner to prioritize protection requirements to accomplish the mission or task.

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



INPUTS

- Higher HQ/Strategic/ Operational Guidance
- Commander’s Planning Guidance
- Previous OPSEC Plans and Assessments
- Intelligence Assessments and Products

OUTPUTS

- OPSEC Staff Estimate
- Essential Secrets/OPSEC Tasks
- OPSEC Mission Statement
- Preliminary CIIL
- OPSEC Threat/Conduit Analysis

Figure 6-5. Mission Analysis Inputs and Operations Security Outputs

It is vital for OPSEC planners to conduct thorough analysis of the operational aspects of an operation. OPSEC planners use operational aspects to focus planning efforts and frame different parts of an operation through friendly force activity mapping and the identification of associated indicators. Viewing the operational aspect in the context of the IE, in sequence, and not as an isolated aspect, allows the OPSEC planner to understand how the adversary may interpret the aspect in relation to other friendly activities or in a broader context, activity, or campaign that is occurring. Figure 6-6 depicts the concept of operational aspects of friendly activities when viewed in isolation, sequence, and context.

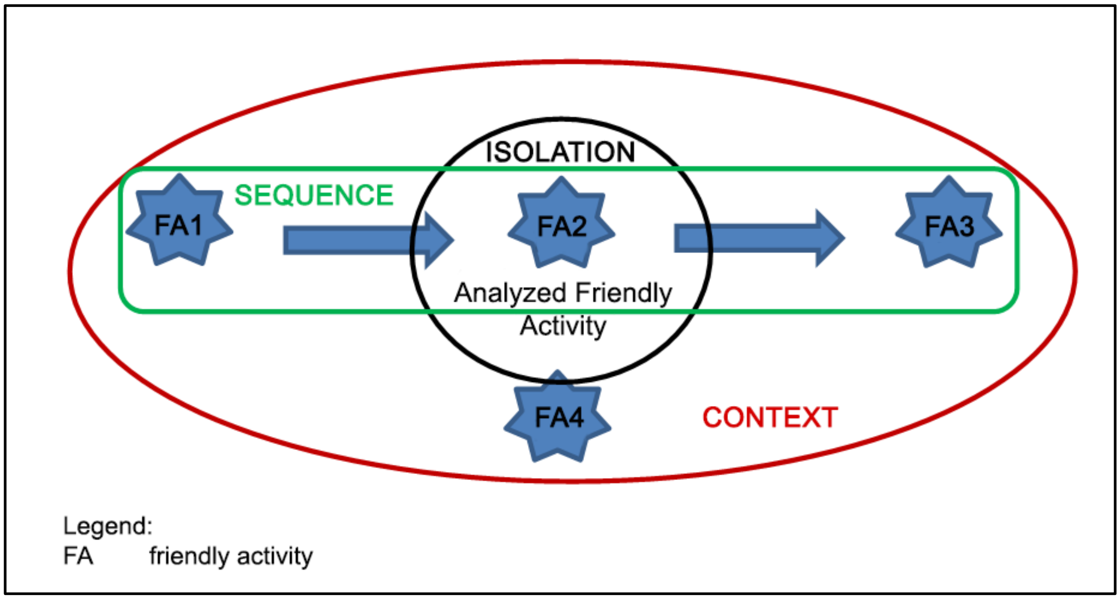


Figure 6-6. Isolation, Sequencing, and Context Perspective

Because each phase of an operation is different and has unique operational requirements, OPSEC planners develop essential secrets for each phase or part of an operation.

1. Example Eessential Secret. The timing, location, and method of a CSG maneuver into the AO.

To turn an essential secret into an OPSEC task, OPSEC planners add a verb (e.g., protect or safeguard). These OPSEC tasks represent the broadest guidance to the staff and subordinate units.

2. Example Operations Security Task. Protect the CII associated with the timing, location, and method of the CSG's maneuver into the AO.

The OPSEC mission statement is derived from OPSEC tasks and provides focus to OPSEC planners and planning teams by answering the questions of who, what, when, where, and why. An OPSEC mission statement may incorporate multiple OPSEC tasks and serves to frame and focus further planning efforts.

3. Example Operations Security Mission Statement. Upon order, commander, task force XX employs OPSEC measures/countermeasures to protect essential secrecy and mitigate operational vulnerabilities associated with timing, location, and method of CSG maneuver into the AO from I day to I+5 day and CSG intent to conduct a flexible response option on I+6 day.

6.6.2 Essential Secrets to Indicators

Once essential secrets are determined, OPSEC planners must conduct a friendly activity analysis to determine if the activities reveal essential secrets to the adversary. Each friendly activity has indicators associated with it. Indicators are friendly detectable events or actions that must happen to execute an activity. These indicators project information into the IE that the adversary could use to derive operational aspects or essential secrets. When conducting friendly activity analysis or mapping, OPSEC planners identify all observable indicators without consideration to the adversary capability. Each activity has unique operational indicators and OPSEC planners consult with other SMEs to ensure all indicators are considered. Indicators can be physical, technical, or administrative. Physical indicators are anything detected by the human senses (e.g., a ship's wake, flight operations, or a submarine periscope). Technical indicators are unique electromagnetic, thermal, acoustic, radiological, or other emanations not readily detected by the human senses (e.g., radar, data or communications signals, ship noise propagation, and magnetic signatures). Specialized equipment is typically required to observe them. Administrative indicators are documents, procedures, or other observable coordination related to friendly activities. Examples include coordination messages (e.g., movement reports, logistic requirements, flight plans, contracts, travel planning, and diplomatic clearances).

The overall summation of indicators and related associations for a particular activity becomes the operational profile, or information derived by the adversary based on all observable indicators. The compilation of indicators for friendly activities is the preliminary CIIL. Unlike a program CIL provided to all users of information in an organization, a preliminary CIIL serves as a planning tool for OPSEC planners to conduct further vulnerability analysis. Figure 6-7 depicts the three types of OPSEC indictors: physical, technical, and administrative.

When conducting friendly activity analysis, OPSEC planners must consider the five characteristics of an indicator: signatures, associations, profiles, contrasts, and exposures (see 3.2). OPSEC planners refer to these characteristics collectively as SAPCE. Often seemingly unimportant or overlooked signatures and associations, if observed by the adversary, can have large impacts in the adversary's understanding of friendly activities and could lead to the compromise of essential secrecy.

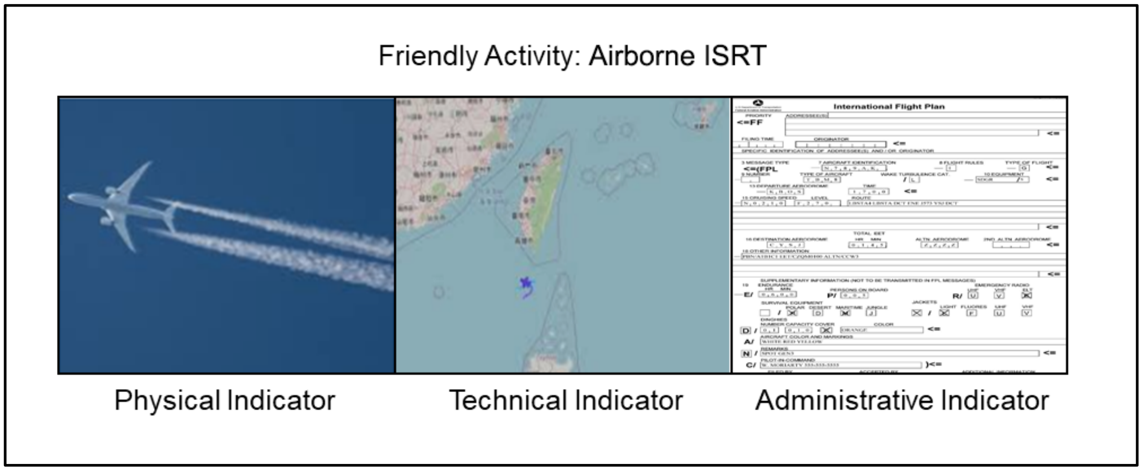


Figure 6-7. Operations Security Indicators

6.6.3 Focus on Adversary Intelligence Collection

An OPSEC program focuses on a large set of adversaries to establish a baseline to protect against potential threats. However, supporting a plan, operation, or mission requires OPSEC planners to focus on a specific adversary and threat analysis. OPSEC planners work closely with intelligence counterparts to understand the adversary's capabilities and intent. Specifically, OPSEC planners must understand the adversary's collection capabilities and systems and how they move, analyze, and store information. This is a much more detailed process of threat analysis than what a standard OPSEC program requires.

When analyzing adversary intelligence collection, consider the adversary decision maker. It is not enough for the adversary to collect information; they must then process, analyze, and disseminate intelligence products. The collected information and subsequent intelligence products often must traverse bureaucratic lines of communication before reaching the adversary decision maker who can act on the intelligence. OPSEC planners must consider the time it takes the adversary to complete these processes. Analyzing the adversary's ability to operate in the IE is known as conduit analysis.

Conduit analysis is an intelligence process for identifying all parts of the adversary's ISRT systems and architecture. Conduits or pathways collect, pass, analyze, and deliver data or information to a decision maker. A typical conduit consists of a sensor, links for transmission, and nodes through which data passes. Not only is conduit analysis a useful tool for OPSEC planners, other IRC planners conducting ISRT, MILDEC, EW, and cyberspace require this intelligence to achieve nonkinetic effects in the IE. Coordination should occur between the supporting intelligence activities and the IW cell or the IW staff. Intelligence products should be disseminated to all planners who require them. Following adversary conduit analysis, OPSEC planners are ready to produce OPSEC staff estimates and conduct vulnerability analysis to support COA development. OPSEC planners present staff estimates to the N39 or IW cell director.

6.7 COURSE OF ACTION DEVELOPMENT, ANALYSIS, AND DECISION

OPSEC planners conduct vulnerability analysis and risk assessment during the COA development and COA wargame/analysis phases of the NPP. As operations planners develop COAs, OPSEC planners conduct vulnerability analysis and risk assessment for each potential COA to determine which indicators could become vulnerabilities within a particular friendly activity. OPSEC vulnerabilities are indicators that are observable through an adversary conduit which the adversary can act upon in time to impact friendly operations. If the adversary cannot observe an indicator, it is not an OPSEC vulnerability. If an indicator is observable, but the adversary does not have time to process and execute a reaction to affect an operation, mission, or task, it is not an OPSEC vulnerability. If the adversary simply lacks the capability to affect an operation, it is not an OPSEC vulnerability. Figure 6-8 depicts OPSEC vulnerabilities as they are observable to the adversary.

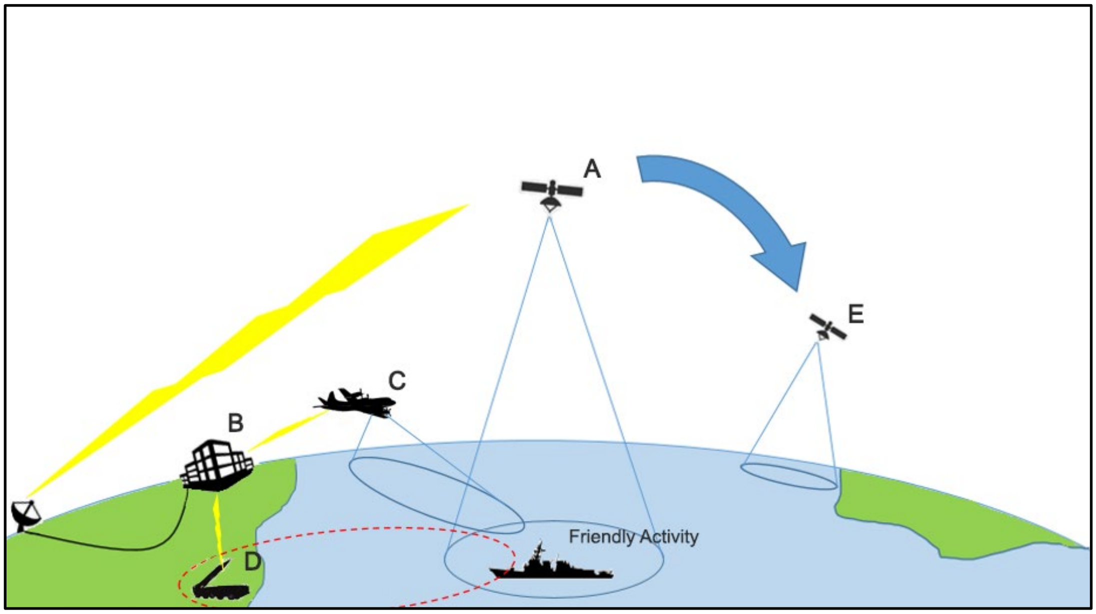


Figure 6-8. Operations Security Vulnerability Vignette

In Figure 6-8, as the adversary overhead sensor (A) moves on station over the friendly activity, physical and technical indicators observed by the sensor are transmitted through the adversary conduit to the headquarter fusion center (B), where an airborne sensor (C) is cued to provide refined targeting data to an engagement asset (D). The physical and technical indicators of the friendly activities are OPSEC vulnerabilities as they are observable to the adversary conduit, and the adversary has the time and capability to affect the friendly activity, even after the original sensor (E) has moved off station.

Once OPSEC planners have identified vulnerabilities, initial risk to mission or force can be determined. Risk is calculated by assessing the probability an adversary would act on a vulnerability and the impact to an operation or mission if that action occurred. If the risk is unacceptable, OPSEC measures/countermeasures are employed to lower the risk to an acceptable level.

OPSEC measures/countermeasures are methods and means to gain and maintain essential secrecy through OPSEC effects. OPSEC measures are means implemented to conceal friendly CII from observation (i.e., things we do to ourselves), while OPSEC countermeasures are the means directed at the adversary conduit (i.e., things we do to the adversary). MOPs and MOEs are created for each measure or countermeasure to assess the implementation or effectiveness.

OPSEC tasks are the execution part of an OPSEC plan. Examples include protect, conceal, safeguard, obfuscate, and mask. OPSEC effects are desired outcomes, phrased in measurable terms of the impact on the adversary. Tasks are formulated to direct the implementation of OPSEC measures/countermeasures to achieve desired effects. This requires significant coordination with other planners to ensure that OPSEC tasks are coordinated and realistically executable.

An example of an OPSEC task: Commander, task force XX will employ EMCON and maneuver to mask technical and physical indicators from adversary overhead collection from I day to I+5 day.

OPSEC tasks can be coordinated in their employment through OPSEC techniques. OPSEC techniques include:

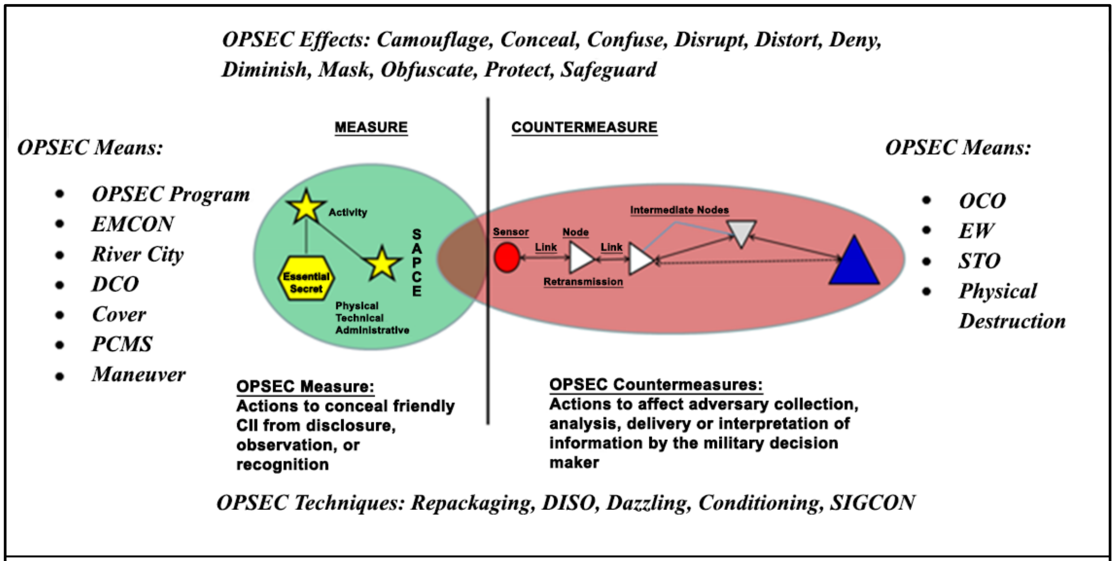
1. Repackaging. Making one profile resemble another existing or new profile by adding or subtracting observable signatures.

2. Dazzling. Creating multiple contrasts in other concurrent activities to draw attention away from the CII that cannot be effectively concealed.

3. Deception in Support of Operations Security. Creating multiple false indicators to make the protected activity harder to interpret by the adversary and protect friendly operations against adversary collection.

4. Conditioning. Introducing and repeating an operational pattern to create a sense of normalcy. The purpose is to create an opportunity for surprise or to induce a contrast, creating a friendly advantage.

Figure 6-9 depicts OPSEC measures/countermeasures.


OPSEC Effects: Camouflage, Conceal, Confuse, Disrupt, Distort, Deny, Diminish, Mask, Obfuscate, Protect, Safeguard
MEASURE
COUNTERMEASURE
OPSEC Means:
OPSEC Program
EMCON
River City
DCO
Cover
PCMS
Maneuver
Activity
Essential Secret
S A P C E
Physical Technical Administrative
Sensor
Node
Link
Link
Intermediate Nodes
Retransmission
OPSEC Means:
OCO
EW
STO
Physical Destruction
OPSEC Measure:
Actions to conceal friendly CII from disclosure, observation, or recognition
OPSEC Countermeasures:
Actions to affect adversary collection, analysis, delivery or interpretation of information by the military decision maker
OPSEC Techniques: Repackaging, DISO, Dazzling, Conditioning, SIGCON

Legend:	
PCMS	passive countermeasure system
STO	special technical operations

Figure 6-9. Operations Security Measures and Countermeasures

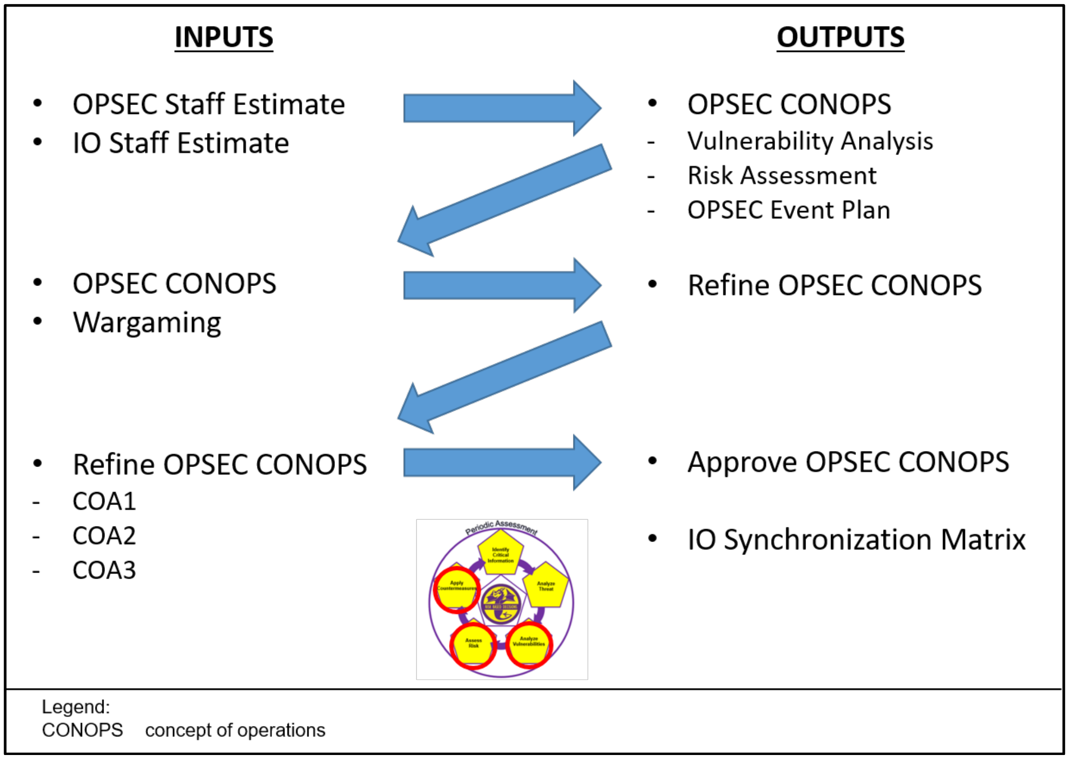
Friendly activities present multiple vulnerabilities that require mitigation through OPSEC means, methods, and techniques. The collection of OPSEC measures/countermeasures is an OPSEC event. OPSEC events have a desired effect and decrease the adversary's ability to derive selected distinguishable operational aspects.

During COA wargaming or the comparison phase of the NPP, OPSEC planners identify and apply OPSEC measures/countermeasures for each COA. This involves developing a concept of operations (CONOPS) for OPSEC activities, tasks, and timeline. OPSEC planners develop the measures/countermeasures that the forces take to achieve essential secrecy. This process is refined until COA approval. Figure 6-10 depicts the OPSEC inputs and outputs of the COA development step of the NPP.

6.8 DEVELOPMENT AND TRANSITION

Once a COA is approved, OPSEC planners translate their work into a section of the OPORD or plan. The OPSEC section of the plan or order is traditionally included as Tab C (Operations Security), to Appendix 3 (Information Operations), of Annex C (Operations). Appendix E provides an example of Tab C.

As part of the OPSEC plan, OPSEC planners develop an assessment plan to measure the effectiveness of OPSEC tasks. Prior to execution, OPSEC assessments are conducted through exercises, war games, or other activities to identify gaps or weakness in the OPSEC plan. Identified gaps are addressed in future iterations of the OPSEC plan.



INPUTS

- OPSEC Staff Estimate
- IO Staff Estimate

OUTPUTS

- OPSEC CONOPS
  - Vulnerability Analysis
  - Risk Assessment
  - OPSEC Event Plan

INPUTS

- OPSEC CONOPS
- Wargaming

OUTPUTS

- Refine OPSEC CONOPS

INPUTS

- Refine OPSEC CONOPS
  - COA1
  - COA2
  - COA3

OUTPUTS

- Approve OPSEC CONOPS
- IO Synchronization Matrix

Legend:
CONOPS concept of operations

Figure 6-10. Course of Action Development, Analysis, and Decision Inputs and Outputs

Examples of MOPs include:

1. Number of COMSEC violations
2. Number of decoys employed
3. Detection of signal leakage.

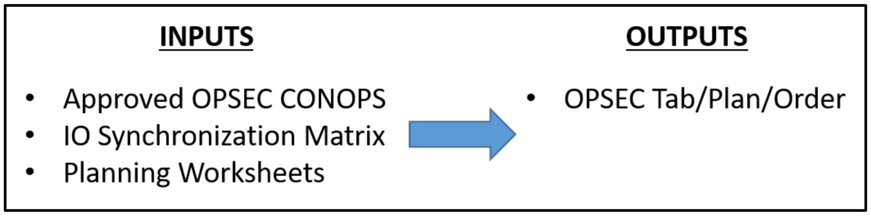
Examples of MOEs include:

1. Increase/decrease of adversary collection assets deployed from I to I+5
2. Increase/decrease of adversary air defense activity from I+5 to I+6
3. Increase/decrease of adversary communication activity from I to I+5.

Possible sources of MOPs/MOEs:

1. Intelligence assessments/reports
2. Open-source research
3. JCMA
4. Own-force monitoring
5. OPSEC assessment team observations.

During the execution of an order, OPSEC planners closely track OPSEC tasks through IO synchronization matrixes, monitor identified MOPs and MOEs, and terminate OPSEC tasks when no longer viable, effective, or required. MOEs requiring intelligence support are coordinated and integrated into collection plans prior to the start of an operation. Figure 6-11 depicts the OPSEC inputs and outputs of the plan/order development step of the NPP.



INPUTS

- Approved OPSEC CONOPS
- IO Synchronization Matrix
- Planning Worksheets

OUTPUTS

- OPSEC Tab/Plan/Order

Figure 6-11. Plan/Order Development Inputs and Outputs

INTENTIONALLY BLANK

APPENDIX A

Identify Critical Information and Indicators

The commander must understand the importance of a positive operations security (OPSEC) culture. This includes appointing a command OPSEC officer (properly trained and designated in writing), implementing a command OPSEC policy, and assigning members to the operations security working group (OWG). Completion of the OPSEC administrative and training requirements are only the prerequisites for developing a robust command OPSEC program. One of the most important responsibilities of an OPSEC officer in managing an OPSEC program is developing a critical information list (CIL). This appendix provides a systematic approach to developing a CIL. Figure A-1 depicts friendly perspective considerations when developing CILs.

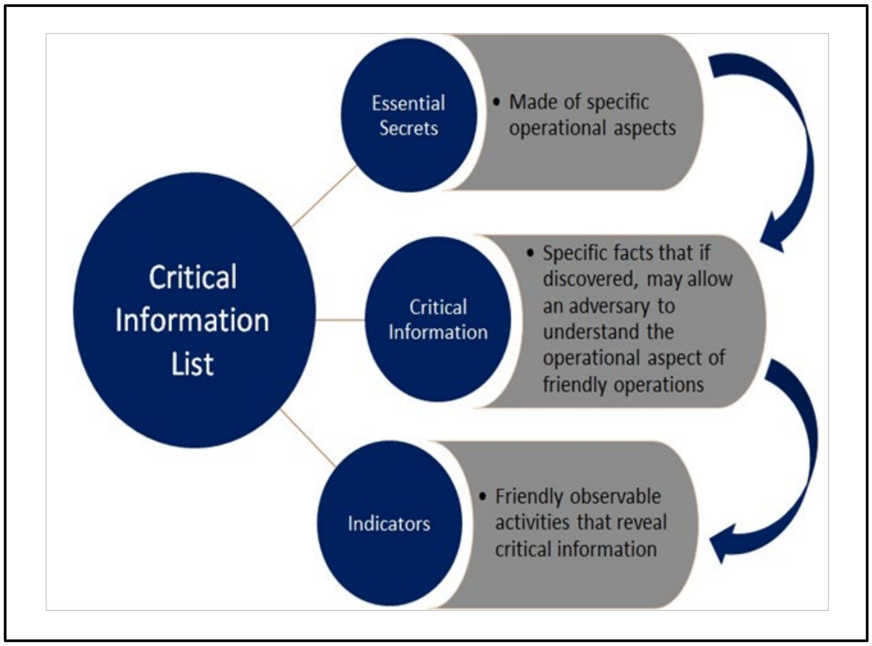

Critical Information List
Essential Secrets
• Made of specific operational aspects
Critical Information
• Specific facts that if discovered, may allow an adversary to understand the operational aspect of friendly operations
Indicators
• Friendly observable activities that reveal critical information

Figure A-1. Friendly Perspective Critical Information List Development

To develop a CIL, OPSEC officers complete the following steps:

1. Step 1. Assemble and train the OWG.

   OPSEC officers cannot and should not try to develop the CIL by themselves. It is imperative representatives from each department, directorate, or section participate. Train the OWG on the eight operational aspects (see 3.1), essential secrets, and indicators for members to gain a solid understanding of the terms and language used. OWG members are encouraged to attend formal training (e.g., the Navy OPSEC course). Understanding how indicators potentially lead to the disclosure of critical information, essential secrets, and operational aspects is an important concept to master. Instruct the OWG to examine activities from the adversary's perspective.

2. Step 2. Identify operational aspects (essential secrets).

   Identify operational aspects that require protection to maintain essential secrecy. The OWG examines all mission areas, functions, and lines of operation or effort that the organization engages in. By identifying operational aspects that require protection, the OWG can focus on identifying the specific critical information and indicators that might expose those aspects. If information cannot be tied back to one or more of the operational aspects, the information is most likely not critical and not an OPSEC concern. Consider the eight operational aspects:

   a. Presence. Current physical or virtual placement within the operational environment. Presence normally requires additional aspects (e.g., strength or intent) to be useful to the adversary decision-making, unless it is a substantial contrast from normal or anticipated friendly activities.

   b. Capability. Resources enabling a force to undertake a particular kind of military action (i.e., what we can do). In OPSEC, capability is an aspect of friendly activity derived from an observable. Capability closely relates to strength.

   c. Strength. The quality or state of being strong; the influence or power possessed by a person, organization, or country. In OPSEC, strength is an aspect of friendly activity and refers to the level or percentage of capability accessible to the force, as measured by what is required to achieve an operational objective or task with an acceptable level of risk.

   d. Intent. What the force must do, and the conditions the force must establish to accomplish the mission. The adversary normally derives friendly intent by combining analysis of friendly policy statements with analysis of friendly force disposition.

   e. Readiness. The ability of military forces to fight and meet the demands of the assigned mission; the state of preparedness. In OPSEC, readiness is a cumulative aspect of friendly activity that refers to the adversary's assessment of our preparedness for a given military action.

   f. Timing (When). The chronological sequencing of planned actions. In OPSEC, timing is an aspect of friendly operations, when correctly interpreted by the adversary, and in conjunction with previous aspects, allows the adversary to potentially prepare for and/or interdict friendly actions.

   g. Location (Where). The projected physical or virtual position where a force acts to achieve a desired effect.

   h. Method. How forces intend to accomplish an objective—the operational approach. If the adversary correctly pieces together the friendly method for achieving an objective, the adversary can develop a plan to seize the initiative at multiple points along our line of effort, thus thwarting mission success or substantially increasing friendly force overall risk/cost.

3. Step 3. Identify critical information and indicators.

   a. Determine specific information tied to identified operational aspects the organization uses, processes, stores, and transmits. View information from two perspectives, friendly and adversarial. From the friendly perspective, critical information requires protection to ensure mission effectiveness. From the adversarial perspective, critical information is what the adversary needs to act effectively against friendly forces. Combine both friendly and adversarial lists, removing duplicate information.

   b. Consider and identify indicators that could expose critical information to adversary collection. Not all critical information has an associated indicator.

4. Step 4. Determine impact.

   Determine the mission impact if the critical information is compromised. Impact can be assessed by the amount of time, cost or resources expended, or loss of material and lives. Define impact by a value and standardize its use throughout the OPSEC cycle. For example, a high value could cost lives, a medium value could cost the command time and resources, or a low value could cost training time.

Figure A-2 is a CIL worksheet to assist OPSEC planners in developing CILs.

<table>
<tr><th colspan="4">Critical Information List Worksheet</th></tr>
<tr><th>Operational Aspects</th><th>Critical Information</th><th>Indicator</th><th>Impact Value</th></tr>
<tr><td></td><td></td><td></td><td></td></tr>
<tr><td></td><td></td><td></td><td></td></tr>
<tr><td></td><td></td><td></td><td></td></tr>
<tr><td></td><td></td><td></td><td></td></tr>
<tr><td></td><td></td><td></td><td></td></tr>
<tr><td></td><td></td><td></td><td></td></tr>
</table>

Figure A-2. Critical Information List Worksheet

The commander approves the CIL and promulgates it for all members of the organization. CILs are concise, easy to understand, and available to all members of the command. It is especially important to review the CIL prior to deployment, upon receipt of a new mission, and when entering a new operating area.

INTENTIONALLY BLANK

APPENDIX B
Threat and Vulnerability Analysis

B.1 THREAT ANALYSIS

This appendix discusses methods to analyze operations security (OPSEC) threats and vulnerabilities.

The first step is to request a threat assessment (TA) from an organization that understands the unit or organization’s potential adversaries.

Analyzing a threat, or the adversary, in the OPSEC cycle includes identifying potential adversaries in the operational environment and their associated capabilities, limitations, and intentions to collect, analyze, and use critical information against friendly forces.

There is no standard format for a TA. Use the standard format or methodologies found through the intelligence functions.

In the threat analysis worksheet (see Figure B-1), the OPSEC officer can assess the adversary’s intent to collect against friendly forces, the level of collection capability possessed by each adversary intelligence discipline, and the overall assessment confidence level. If the assessment states a high confidence in a threat capability, then consider it proven. If the assessment states a low confidence in a threat capability, then identify it as estimated. Derive an overall threat rating by multiplying the adversary intent and capability.

[Adversary Intent] x [Collection Capability] = [Overall Threat Rating]

If the adversary has allies or friends that may provide collection support, add them as a threat to the operation and complete the third party information suppliers section of the threat analysis worksheet.

B.1.1 U.S. Intelligence Community Resources

There are many agencies and resources available through the U.S. intelligence community. The following agencies are potential sources that can inform the OPSEC threat analysis process.

All OPSEC officers start with their organic or higher headquarters’ intelligence shop. The intelligence shop has access to all-source intelligence feeds and personnel who understand the organization’s mission and the adversaries that can collect against it.

Naval Criminal Investigative Service (NCIS) fulfills the investigative and counterintelligence (CI) needs of the Navy and Marine Corps. NCIS ensures that the commands it supports have the most accurate and relevant intelligence required to protect themselves from terrorism and sabotage threats, criminal and cyber threats, and foreign intelligence collection. NCIS produces local TA products that many OPSEC officers find useful.

Office of Naval Intelligence (ONI) provides maritime intelligence products to the Department of the Navy (DON) and Department of Defense (DOD). ONI specializes in the analysis, production, and dissemination of vital, timely, and accurate scientific, technical, geopolitical, and military intelligence information. The Nimitz Operational Intelligence Center is the primary source for ONI products.

Threat Analysis Worksheet				
Our Mission:				
[Adversary Intent] X [Collection Capability] = [Overall Threat Assessment]				
Primary Adversary				
Intent	Collection Capabilities			Overall Assessment
Estimate of probability adversary will act against us (circle one): High Medium High Medium Medium Low Low	Intelligence Discipline	Circle One:	Level (H/MH/M/ML/L):	Level (H/MH/M/ML/L):
	OSINT	Proven/Estimate/NA		
	HUMINT	Proven/Estimate/NA		
	SIGINT	Proven/Estimate/NA		
	GEOINT	Proven/Estimate/NA		
	MASINT	Proven/Estimate/NA		
Third Party Information Suppliers				
Intent	Collection Capabilities			Overall Assessment
Estimate of probability adversary will act against us (circle one): High Medium High Medium Medium Low Low	Intelligence Discipline	Circle One:	Level (H/MH/M/ML/L):	Level (H/MH/M/ML/L):
	OSINT	Proven/Estimate/NA		
	HUMINT	Proven/Estimate/NA		
	SIGINT	Proven/Estimate/NA		
	GEOINT	Proven/Estimate/NA		
	MASINT	Proven/Estimate/NA		
Legend: H high L low	M medium MH medium high	ML medium low NA not applicable		

Figure B-1. Threat Analysis Worksheet

The Defense Intelligence Agency (DIA) is a DOD combat support agency that is a major producer and manager of foreign military intelligence. The DIA provides military intelligence to warfighters, defense policymakers, and force planners in the DOD and the intelligence community in support of U.S. military planning and operations and weapon systems acquisition.

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

The Central Intelligence Agency keeps the nation safe by preempting threats and furthering U.S. national security objectives by collecting intelligence and producing objective all-source analysis products (e.g., the World Intelligence Review), which provides information that is helpful to threat analysis.

The United States Department of State provides region-specific intelligence on international crime and terrorism threats to U.S. personnel and interests. Units and commands that deploy to foreign soil can benefit from their valuable resources (e.g., country reports on terrorism and official travel warnings).

B.2 VULNERABILITY ANALYSIS

This step requires the operations security working group (OWG) to think like the adversary to determine how susceptible critical information is to adversary collection. The OWG examines how the command stores, transmits, and handles critical information and identifies how potential adversaries may collect that information. Use OPSEC assessments to identify and validate vulnerabilities. Figure B-2 is a vulnerability analysis worksheet.

Vulnerability Analysis Worksheet	
Vulnerability	**Collection Method** **(OSINT, GEOINT, HUMINT, SIGINT, MASINT)**

Figure B-2. Vulnerability Analysis Worksheet

INTENTIONALLY BLANK

APPENDIX C

Risk Assessment and Countermeasure Considerations

C.1 ASSESS RISK

In operations security (OPSEC), risk is a measure of probability that the adversary will be successful in collecting critical information and the resulting cost to the mission. OPSEC officers use a risk assessment worksheet to complete an assessment and readily translate the findings to identify and prioritize appropriate measures/countermeasures. Figure C-1 is an example of a risk assessment worksheet.

Vulnerability	Threat	Threat Rating	Critical Information	Value/ Impact	Risk	Measure/ Countermeasure	Residual Risk

Figure C-1. Risk Analysis Worksheet

Assess initial risk for each vulnerability by using the threat collection capability value and multiplying it by the value of the critical information.

[Threat Assessment Value] x [Impact (Critical Information Value)] = [Risk]

Remain consistent in the use of rating values (e.g., high, medium, low, etc.).

Measures/countermeasures lower the risk level by making vulnerabilities less susceptible to adversary collection. The remaining risk is considered a residual risk.

C.2 MEASURES AND COUNTERMEASURES CONSIDERATIONS

OPSEC measures/countermeasures prevent an adversary from detecting critical information or indicators, provide an alternative interpretation of critical information or indicators (deception), or deny or degrade the adversary's collection capability. Implement measures/countermeasures to mitigate risk, and coordinate and integrate with other information-related capability, security disciplines, and other functions, if applicable.

Prior to recommending measures/countermeasures, the OPSEC officer must carefully consider cost and other impacts that may degrade mission performance. Measures/countermeasures must provide benefits that outweigh the cost. Some considerations include, but are not limited to:

1. Monetary costs that exceed the impact of the loss of critical information.

2. Increased wear and tear on equipment or increased consumption of fuel or other resources.

3. Constraints due to the use of civilian or contractor workforces.

4. Does the measure/countermeasure create another indicator or vulnerability?

5. Is the implementation achievable and measurable?

6. How long is the measures/countermeasures required and what is the termination plan?

OPSEC measures/countermeasures can be anything that works. Sometimes a simple, low-cost solution is the most effective (e.g., proper safeguarding, limiting distribution, and shredding information when no longer needed). Other examples of low-cost OPSEC measures include:

1. Apply appropriate markings to information destined for dissemination.

2. Control trash (e.g., 100 percent shred policy).

3. Disseminate the unit critical information list to all members of the unit.

4. Perform OPSEC training and briefings.

5. Use concealment and physical camouflage.

6. Vary routines.

Technical measures/countermeasures can include:

1. Use secure communications and encryption.

2. Emission control (EMCON).

3. River City.

4. Electromagnetic warfare capabilities.

5. Deception.

Measures of performance (MOPs) and measures of effectiveness (MOEs) help to determine the cost trade-offs of implementing OPSEC measures/countermeasures.

An MOP is a measurement of a measure's/countermeasure's execution. For example, a ship sets EMCON. The MOP would be: EMCON was set per Navy standards and local standard operating procedures; own-force monitoring detected no emanations from the ship.

An MOE is a measurement of whether or not the measure/countermeasure achieved the desired result. Using the same example of setting EMCON, a successful MOE would be: the intelligence reflects the adversary has lost contact on the ship.

Figure C-2 provides a worksheet to capture OPSEC measures/countermeasures and associated MOPs and MOEs.

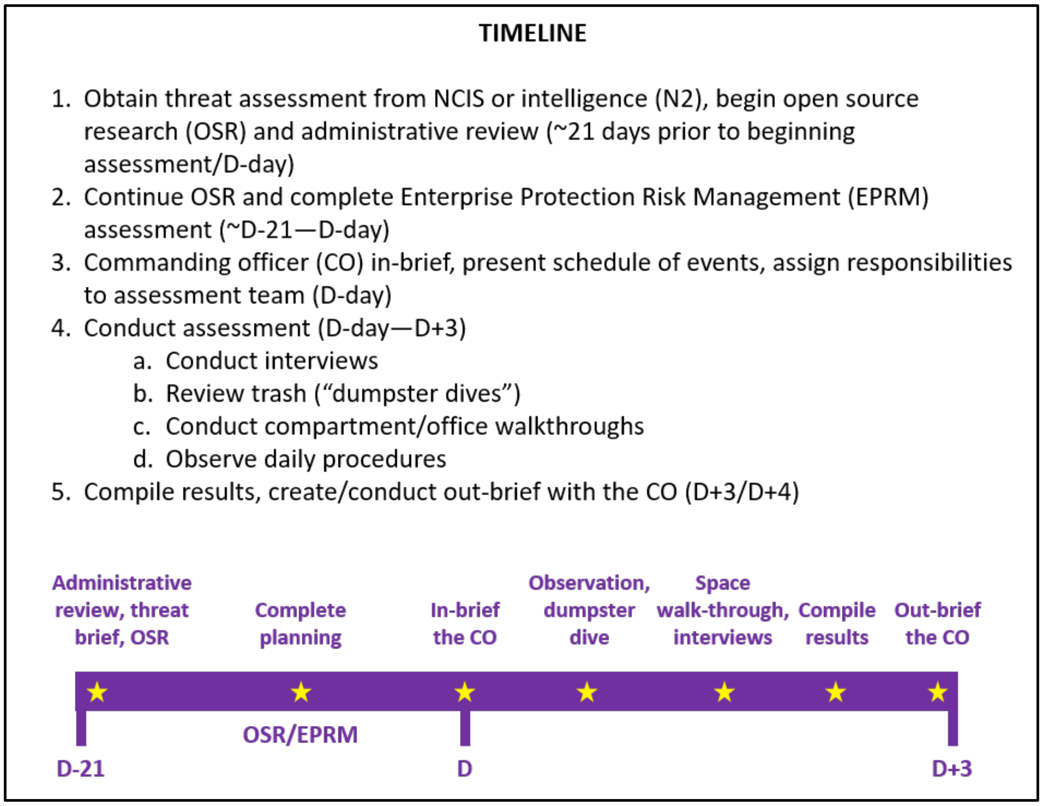
Vulnerability	Countermeasure	MOP	MOE

Figure C-2. Measures and Countermeasures Development Worksheet

APPENDIX D

Internal Assessment Procedures

Used throughout the Department of Defense (DOD), the steps listed in Figure D-1 provide a guide for achieving positive results during the assessment process. First, read all the steps to gain insight into the entire process prior to execution. Although there is no specific or unique training on how to conduct an assessment, a best practice for success is ensuring the operations security (OPSEC) officer attends the Navy OPSEC course and the operations security working group (OWG) members complete, at a minimum, basic OPSEC training.



TIMELINE

1. Obtain threat assessment from NCIS or intelligence (N2), begin open source research (OSR) and administrative review (~21 days prior to beginning assessment/D-day)
2. Continue OSR and complete Enterprise Protection Risk Management (EPRM) assessment (~D-21—D-day)
3. Commanding officer (CO) in-brief, present schedule of events, assign responsibilities to assessment team (D-day)
4. Conduct assessment (D-day—D+3)
   a. Conduct interviews
   b. Review trash (“dumpster dives”)
   c. Conduct compartment/office walkthroughs
   d. Observe daily procedures
5. Compile results, create/conduct out-brief with the CO (D+3/D+4)

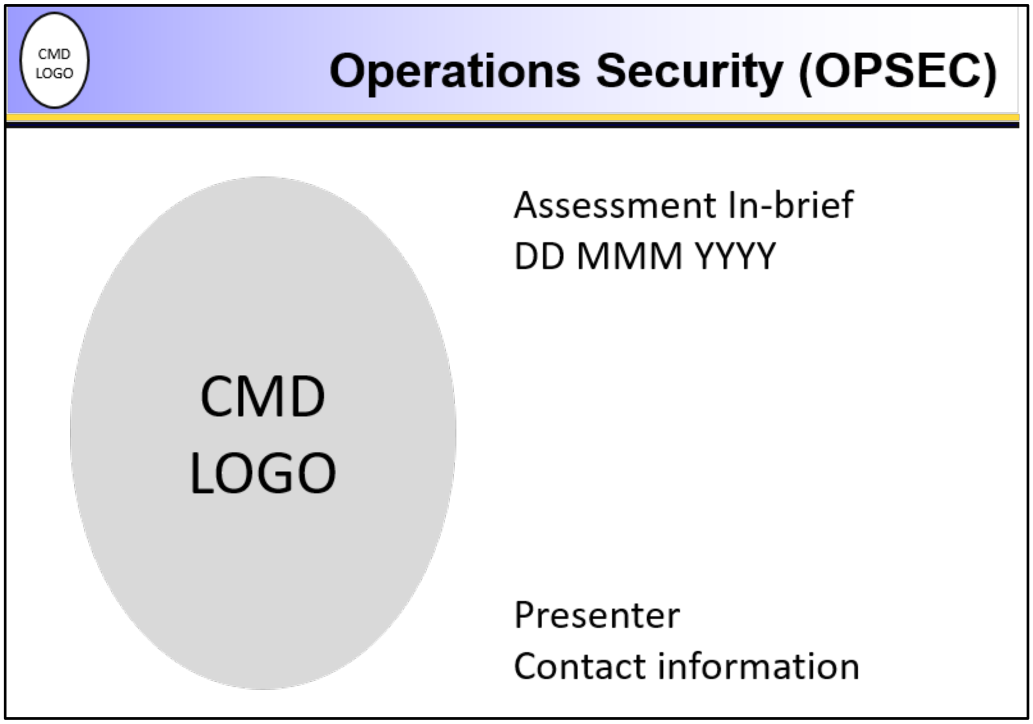
Administrative review, threat brief, OSR
Complete planning
In-brief the CO
Observation, dumpster dive
Space walk-through, interviews
Compile results
Out-brief the CO
OSR/EPRM
D-21
D
D+3

Figure D-1. Example Assessment Timeline

The OPSEC officer and OWG team develop a timeline or a plan of action and milestones, provide an in-brief to the commander, and obtain approval to conduct an internal OPSEC assessment. Figures D-2 through D-9 depict an example in-brief template.

Assign team leads for the different assessment areas (e.g., trash reviews, command member interviews, observations) and use the templates in Figures D-10 through D-13. The templates are available to download from the Naval Operations Security Support Team (NOST) page located at: https://www.navifor.usff.navy.mil/opsec.

Upon assessment completion, compile the results and develop a comprehensive report and an executive brief for the commander. Highlight the vulnerabilities and the measures/countermeasures recommendations (see Figures D-14 through D-24). For additional assistance, contact the NOST at NAVY_OPSEC@us.navy.mil or visit the website at: https://www.navifor.usff.navy.mil/opsec.



CMD LOGO

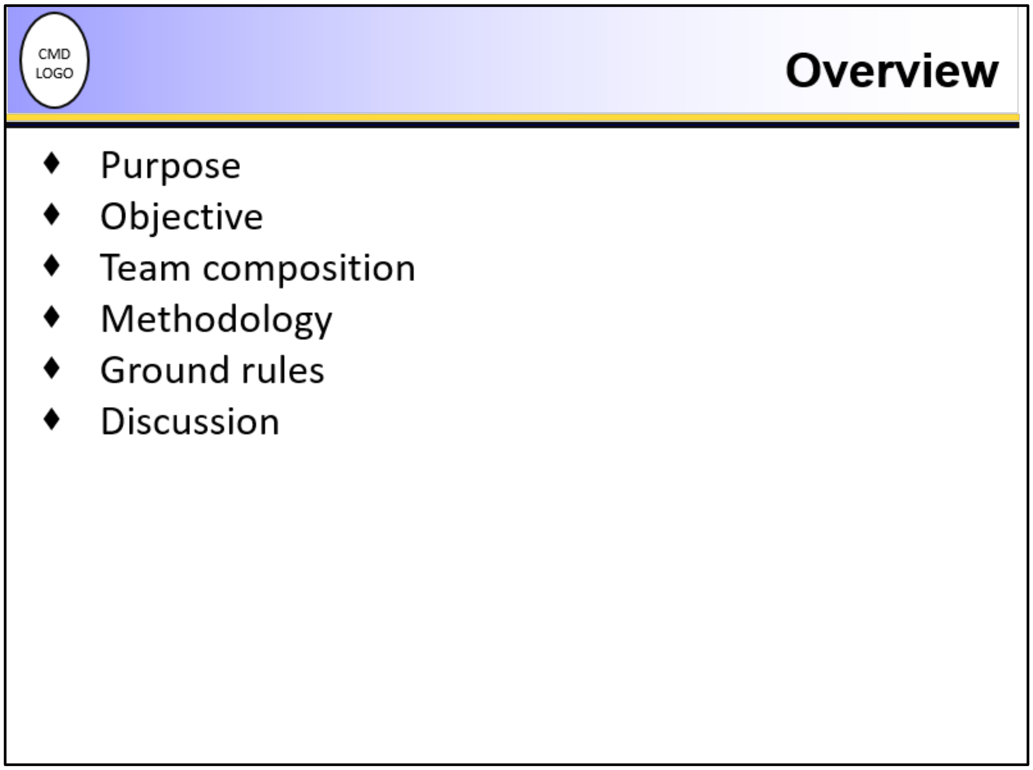
Operations Security (OPSEC)

CMD LOGO

Assessment In-brief
DD MMM YYYY

Presenter
Contact information

Figure D-2. Example Operations Security In-brief: Cover

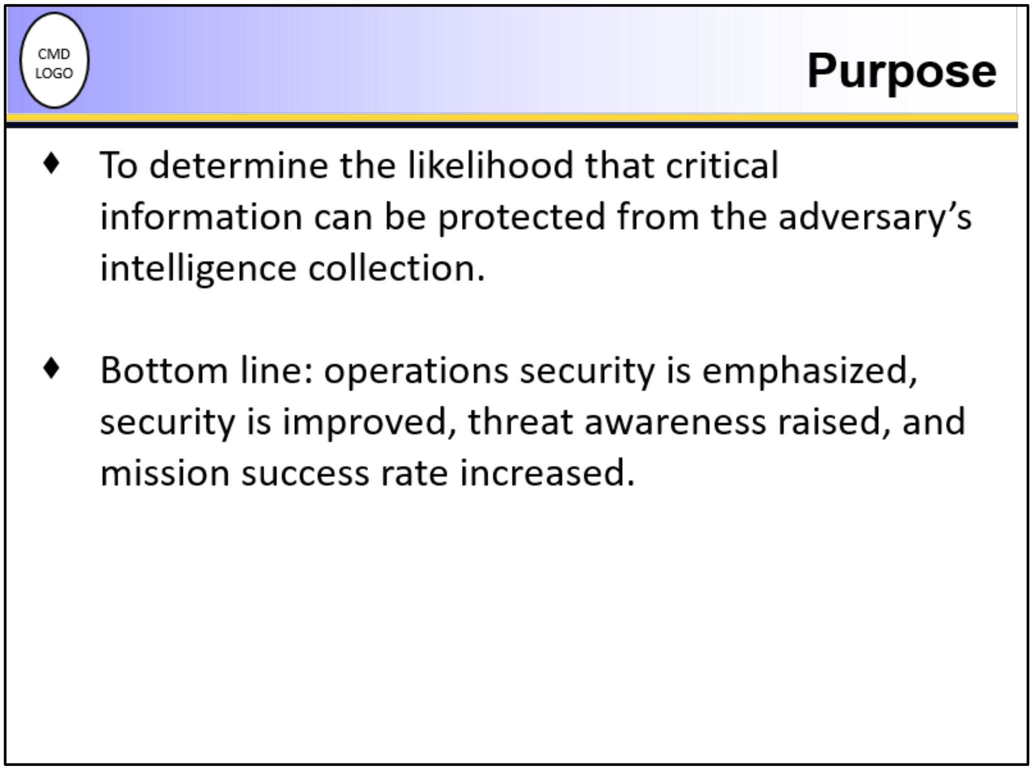


CMD LOGO

Overview

- Purpose
- Objective
- Team composition
- Methodology
- Ground rules
- Discussion

Figure D-3. Example Operations Security In-brief: Overview



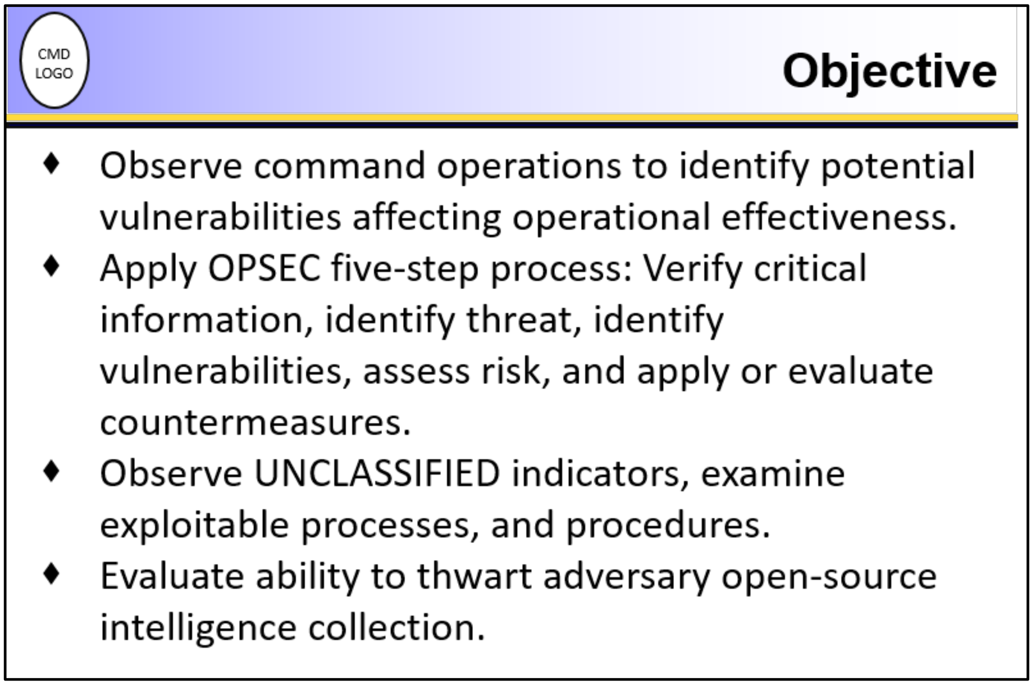
CMD LOGO

Purpose

- To determine the likelihood that critical information can be protected from the adversary's intelligence collection.

- Bottom line: operations security is emphasized, security is improved, threat awareness raised, and mission success rate increased.

Figure D-4. Example Operations Security In-brief: Purpose

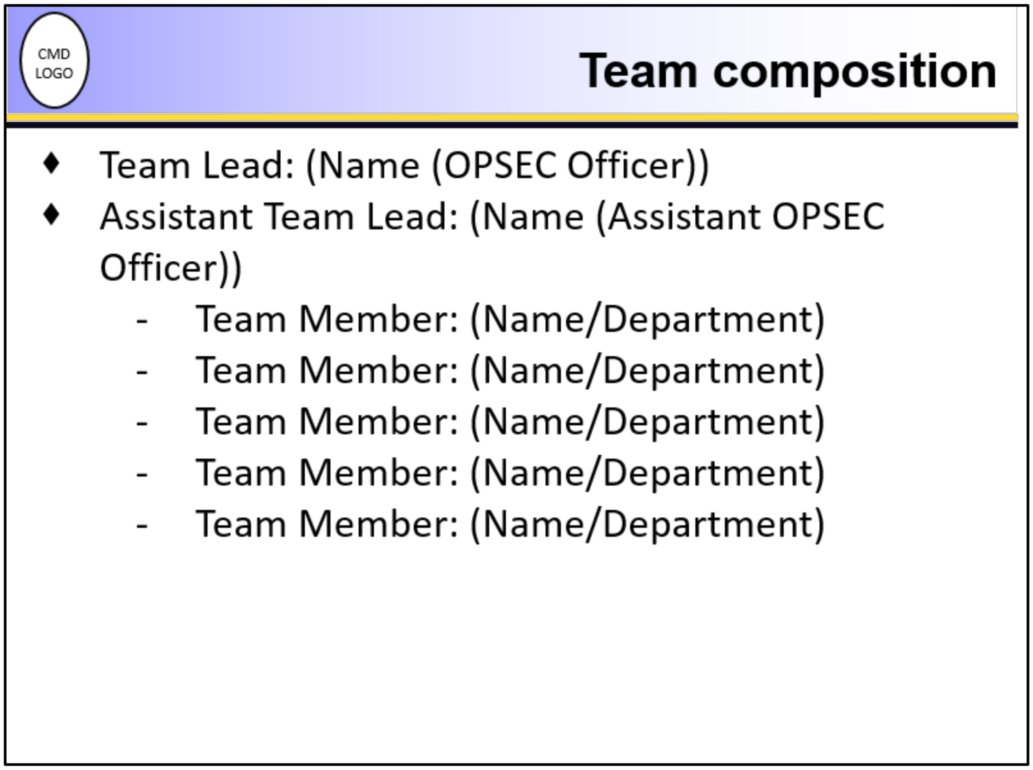


CMD LOGO

Objective

- Observe command operations to identify potential vulnerabilities affecting operational effectiveness.
- Apply OPSEC five-step process: Verify critical information, identify threat, identify vulnerabilities, assess risk, and apply or evaluate countermeasures.
- Observe UNCLASSIFIED indicators, examine exploitable processes, and procedures.
- Evaluate ability to thwart adversary open-source intelligence collection.

Figure D-5. Example Operations Security In-brief: Objective

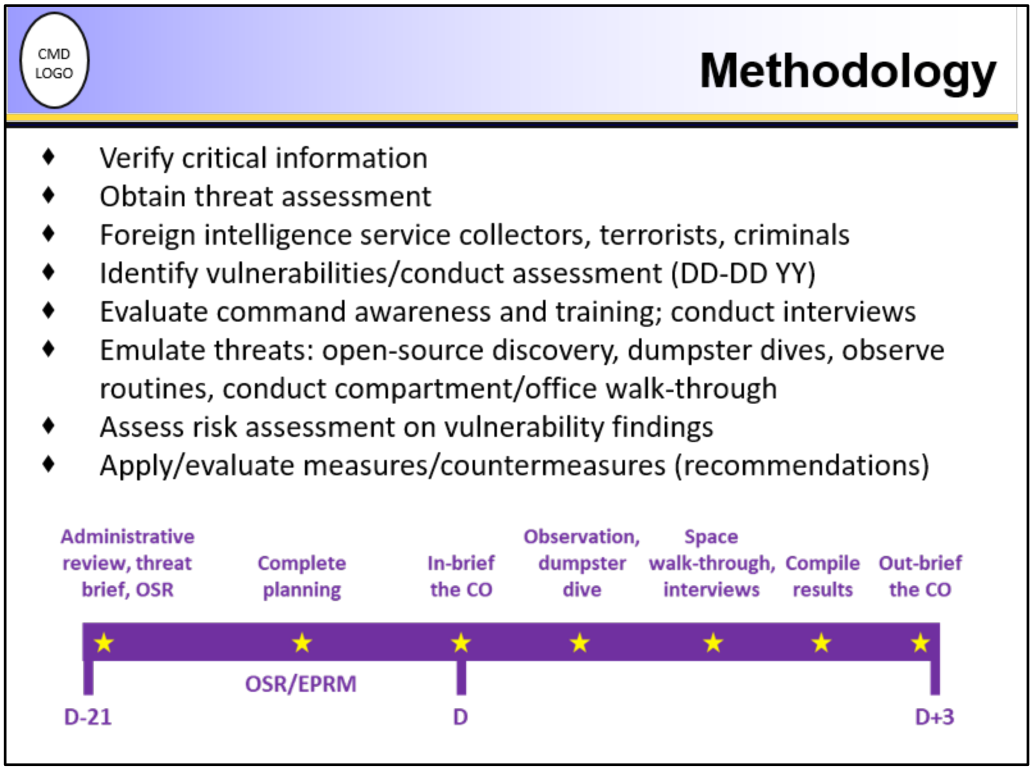


CMD LOGO

Team composition

- Team Lead: (Name (OPSEC Officer))
- Assistant Team Lead: (Name (Assistant OPSEC Officer))
    - Team Member: (Name/Department)
    - Team Member: (Name/Department)
    - Team Member: (Name/Department)
    - Team Member: (Name/Department)
    - Team Member: (Name/Department)

Figure D-6. Example Operations Security In-brief: Team Composition



CMD LOGO

Methodology

- Verify critical information
- Obtain threat assessment
- Foreign intelligence service collectors, terrorists, criminals
- Identify vulnerabilities/conduct assessment (DD-DD YY)
- Evaluate command awareness and training; conduct interviews
- Emulate threats: open-source discovery, dumpster dives, observe routines, conduct compartment/office walk-through
- Assess risk assessment on vulnerability findings
- Apply/evaluate measures/countermeasures (recommendations)

Administrative review, threat brief, OSR

Complete planning

In-brief the CO

Observation, dumpster dive

Space walk-through, interviews

Compile results

Out-brief the CO

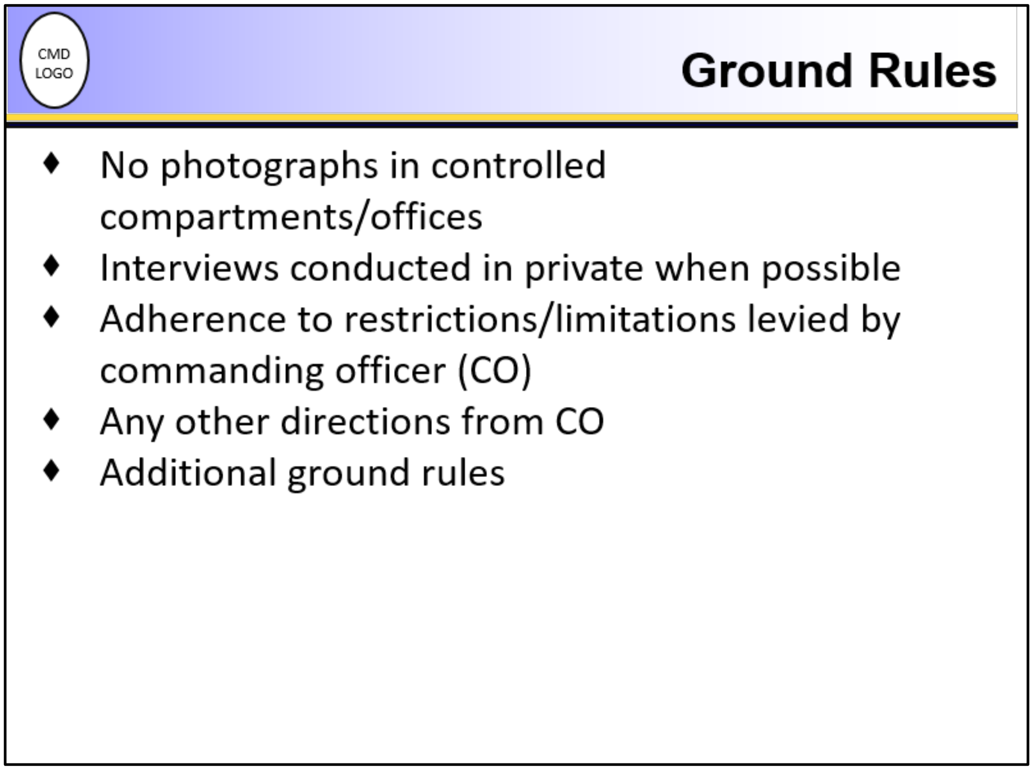
OSR/EPRM

D-21

D

D+3

Figure D-7. Example Operations Security In-brief: Methodology

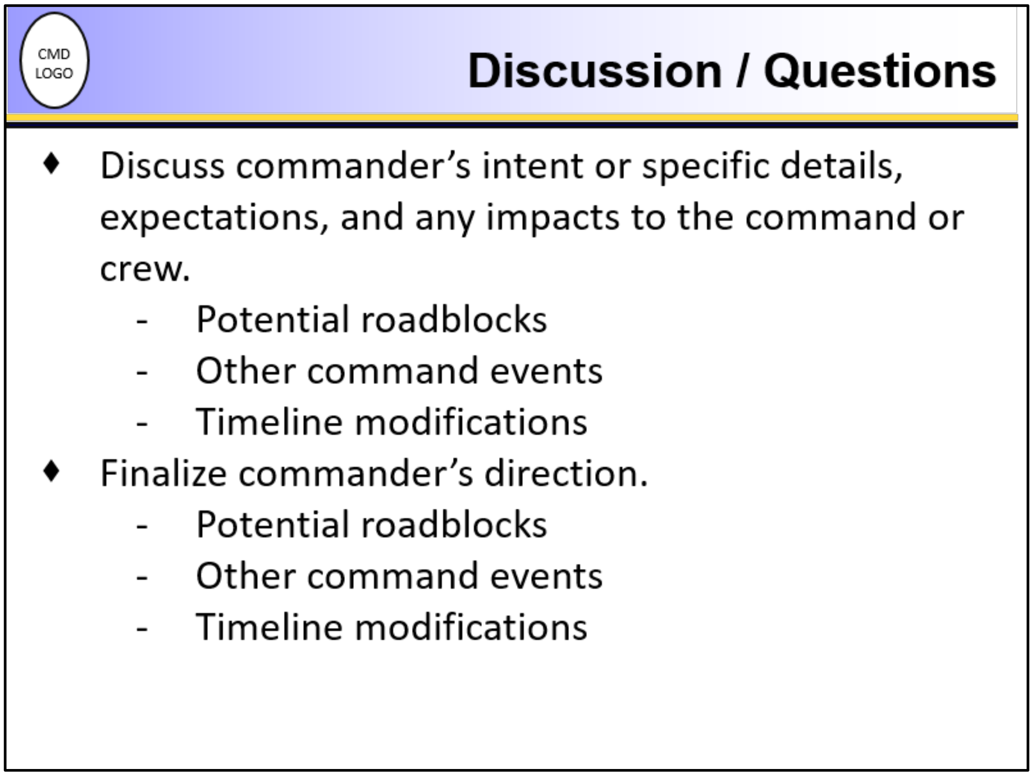


CMD LOGO

Ground Rules

- No photographs in controlled compartments/offices
- Interviews conducted in private when possible
- Adherence to restrictions/limitations levied by commanding officer (CO)
- Any other directions from CO
- Additional ground rules

Figure D-8. Example Operations Security In-brief: Ground Rules

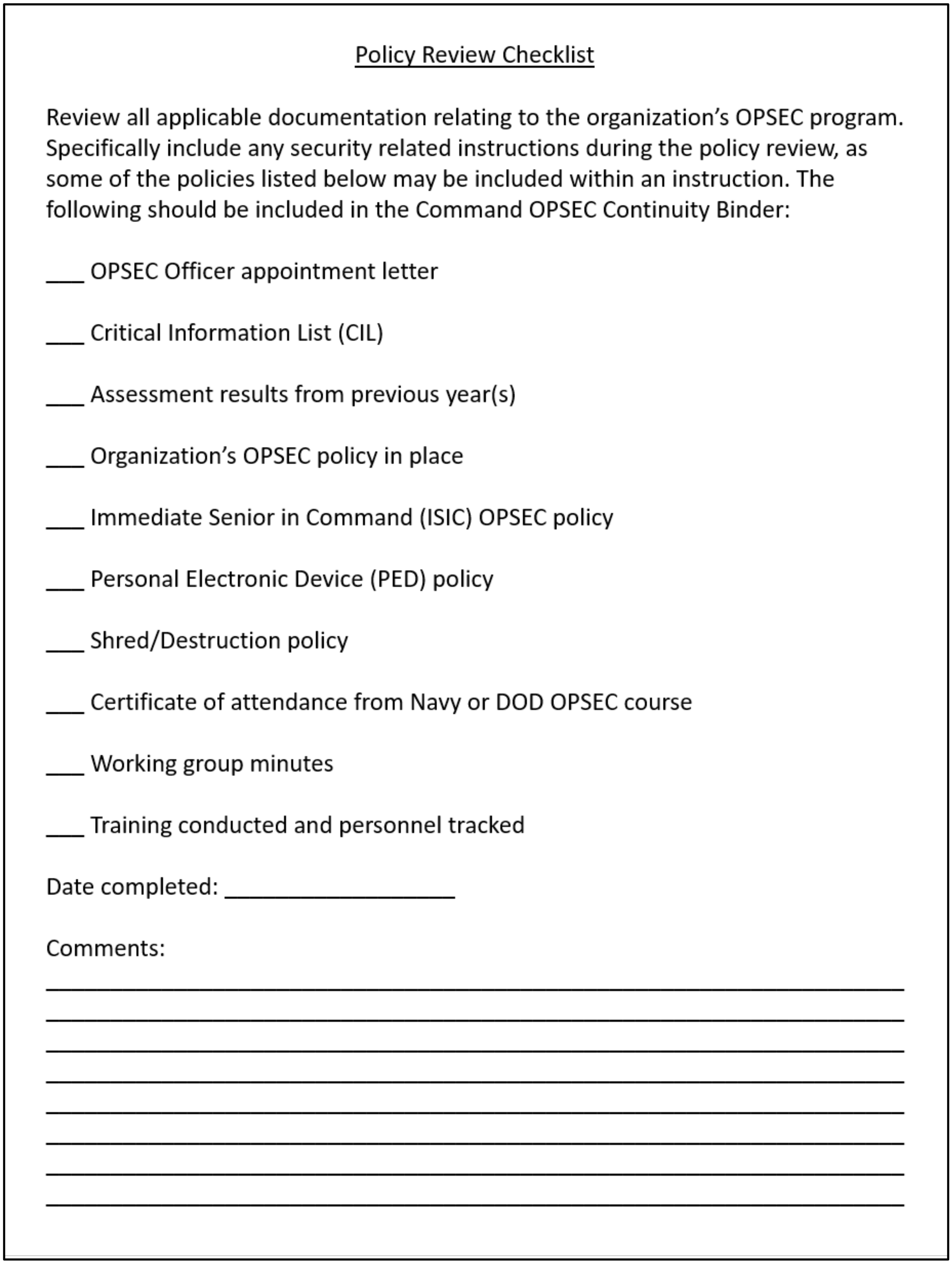


CMD LOGO

Discussion / Questions

- Discuss commander’s intent or specific details, expectations, and any impacts to the command or crew.
  - Potential roadblocks
  - Other command events
  - Timeline modifications
- Finalize commander’s direction.
  - Potential roadblocks
  - Other command events
  - Timeline modifications

Figure D-9. Example Operations Security In-brief: Questions/Discussion



Policy Review Checklist

Review all applicable documentation relating to the organization's OPSEC program. Specifically include any security related instructions during the policy review, as some of the policies listed below may be included within an instruction. The following should be included in the Command OPSEC Continuity Binder:

___ OPSEC Officer appointment letter

___ Critical Information List (CIL)

___ Assessment results from previous year(s)

___ Organization's OPSEC policy in place

___ Immediate Senior in Command (ISIC) OPSEC policy

___ Personal Electronic Device (PED) policy

___ Shred/Destruction policy

___ Certificate of attendance from Navy or DOD OPSEC course

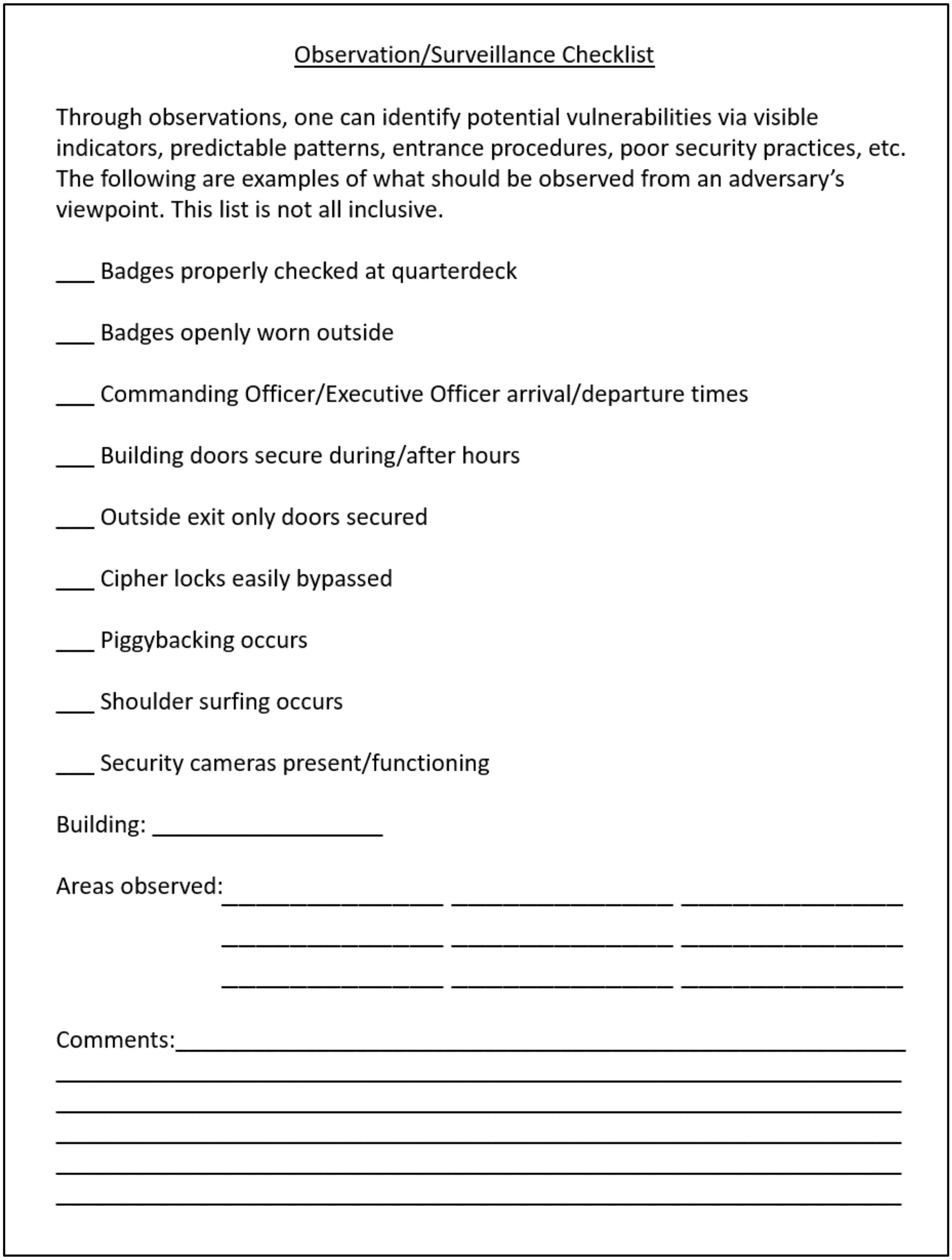
___ Working group minutes

___ Training conducted and personnel tracked

Date completed: ____________________

Comments:
____
____
____
____
____
____
____
____

Figure D-10. Example Policy Review Checklist



Observation/Surveillance Checklist

Through observations, one can identify potential vulnerabilities via visible indicators, predictable patterns, entrance procedures, poor security practices, etc. The following are examples of what should be observed from an adversary's viewpoint. This list is not all inclusive.

___ Badges properly checked at quarterdeck

___ Badges openly worn outside

___ Commanding Officer/Executive Officer arrival/departure times

___ Building doors secure during/after hours

___ Outside exit only doors secured

___ Cipher locks easily bypassed

___ Piggybacking occurs

___ Shoulder surfing occurs

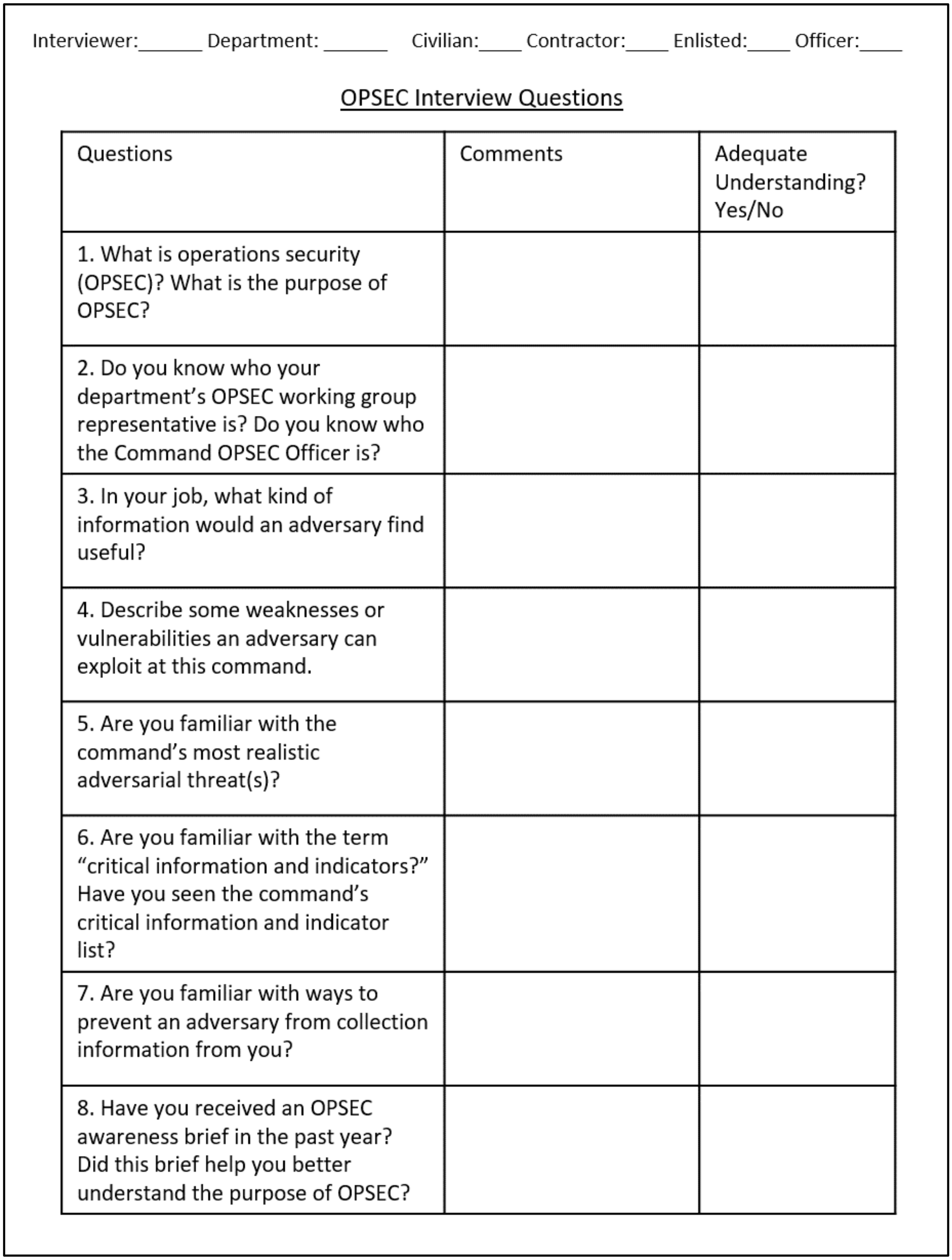
___ Security cameras present/functioning

Building: ____________________

Areas observed: ____________________ ____________________ ____________________
____________________ ____________________ ____________________
____________________ ____________________ ____________________

Comments:____
____
____
____
____
____

Figure D-11. Example Observation Checklist

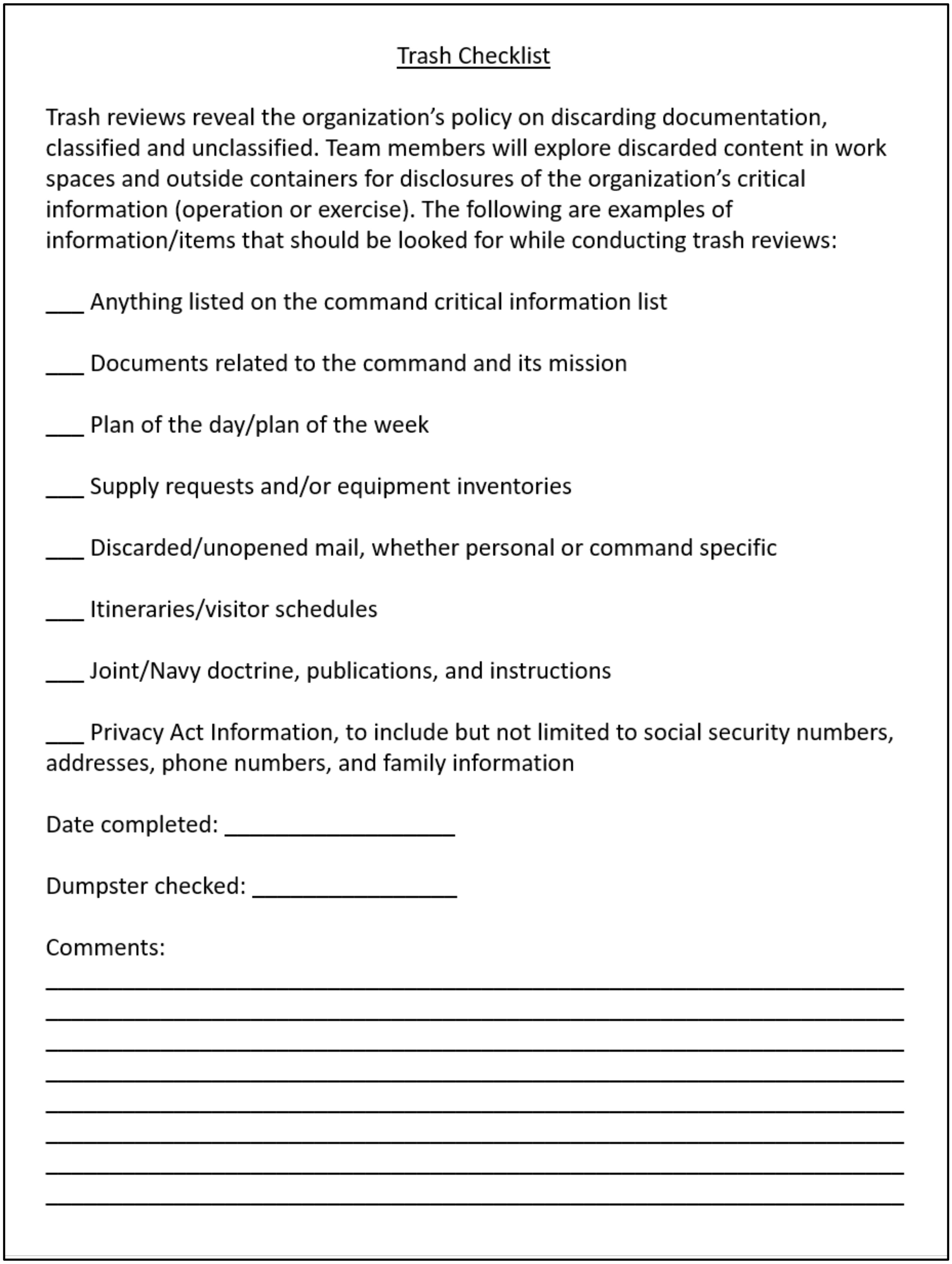


Interviewer:______ Department: ______ Civilian:____ Contractor:____ Enlisted:____ Officer:____

OPSEC Interview Questions

Questions	Comments	Adequate Understanding? Yes/No
1. What is operations security (OPSEC)? What is the purpose of OPSEC?		
2. Do you know who your department's OPSEC working group representative is? Do you know who the Command OPSEC Officer is?		
3. In your job, what kind of information would an adversary find useful?		
4. Describe some weaknesses or vulnerabilities an adversary can exploit at this command.		
5. Are you familiar with the command's most realistic adversarial threat(s)?		
6. Are you familiar with the term "critical information and indicators?" Have you seen the command's critical information and indicator list?		
7. Are you familiar with ways to prevent an adversary from collection information from you?		
8. Have you received an OPSEC awareness brief in the past year? Did this brief help you better understand the purpose of OPSEC?		

Figure D-12. Example Interview Questions



Trash Checklist

Trash reviews reveal the organization's policy on discarding documentation, classified and unclassified. Team members will explore discarded content in work spaces and outside containers for disclosures of the organization's critical information (operation or exercise). The following are examples of information/items that should be looked for while conducting trash reviews:

___ Anything listed on the command critical information list

___ Documents related to the command and its mission

___ Plan of the day/plan of the week

___ Supply requests and/or equipment inventories

___ Discarded/unopened mail, whether personal or command specific

___ Itineraries/visitor schedules

___ Joint/Navy doctrine, publications, and instructions

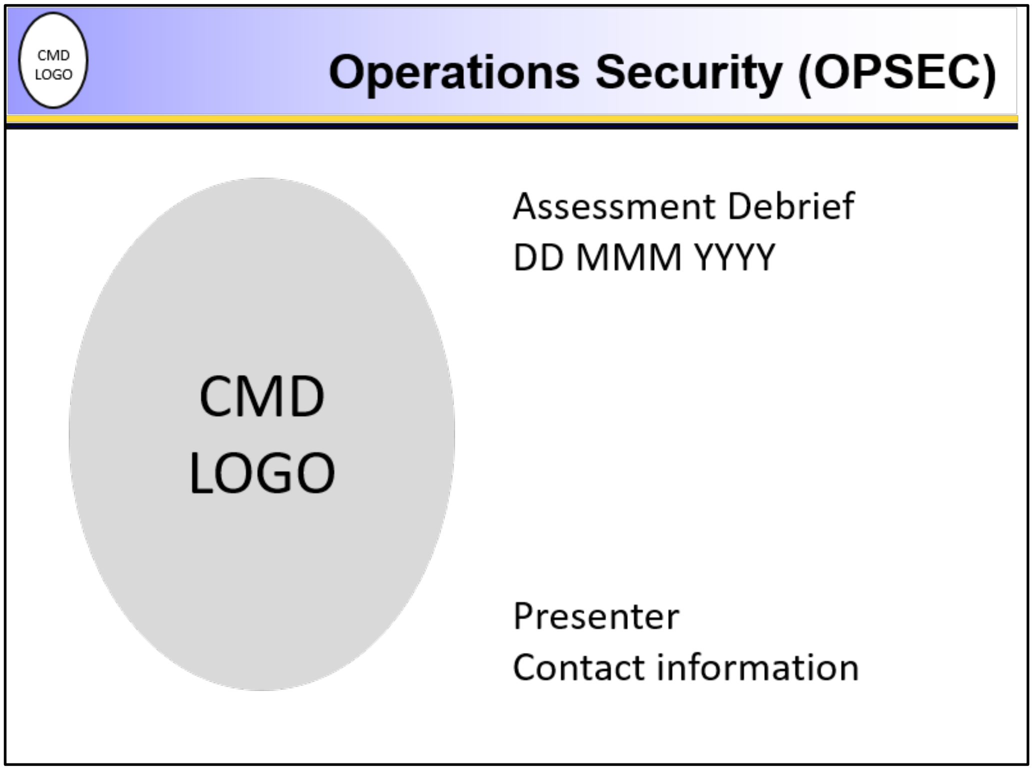
___ Privacy Act Information, to include but not limited to social security numbers, addresses, phone numbers, and family information

Date completed: ___________________

Dumpster checked: _________________

Comments:
____
____
____
____
____
____
____
____

Figure D-13. Example Trash Inspection Checklist



CMD LOGO

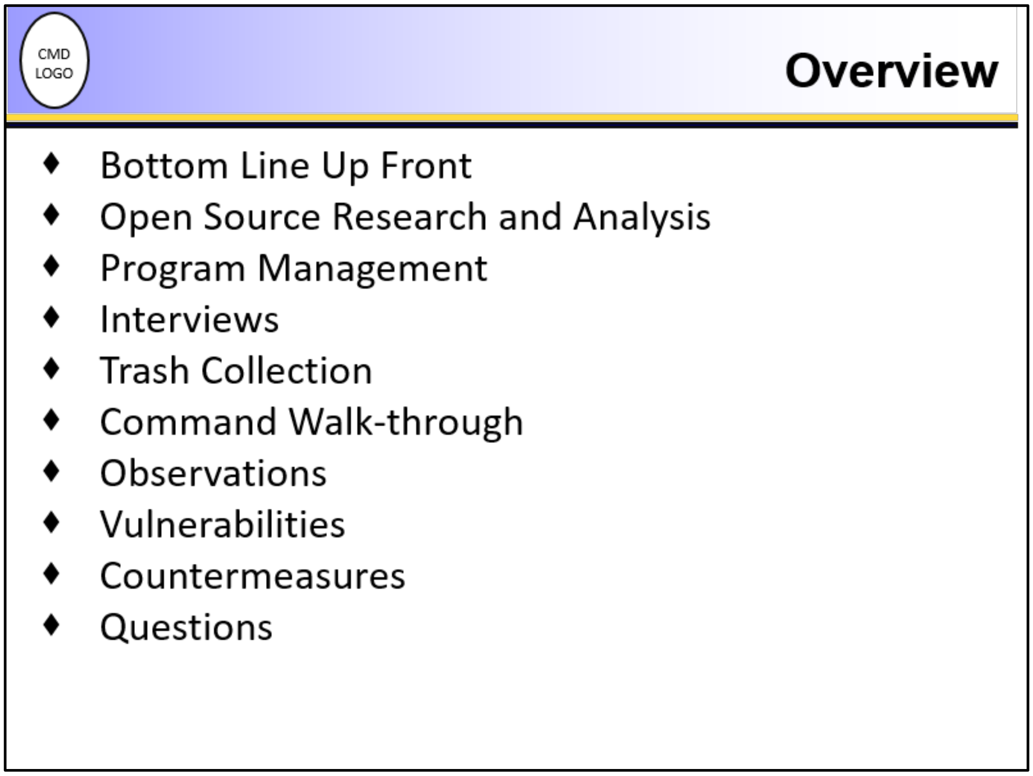
Operations Security (OPSEC)

CMD LOGO

Assessment Debrief
DD MMM YYYY

Presenter
Contact information

Figure D-14. Example Operations Security Debrief: Cover

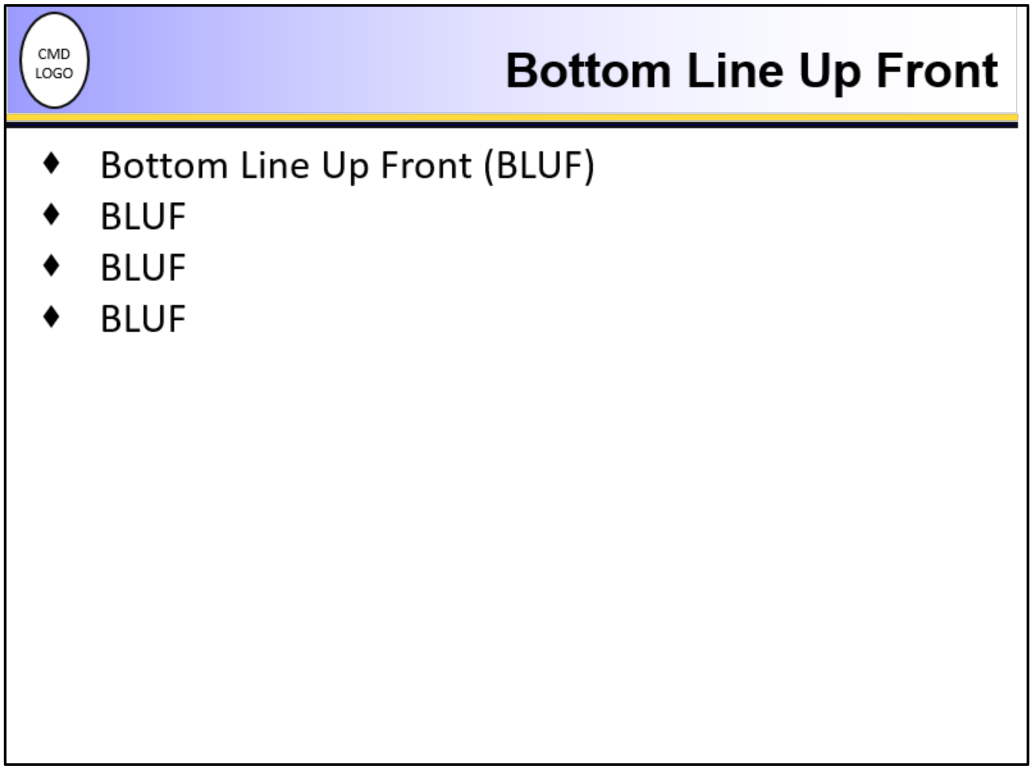


CMD LOGO

Overview

- Bottom Line Up Front
- Open Source Research and Analysis
- Program Management
- Interviews
- Trash Collection
- Command Walk-through
- Observations
- Vulnerabilities
- Countermeasures
- Questions

Figure D-15. Example Operations Security Debrief: Overview

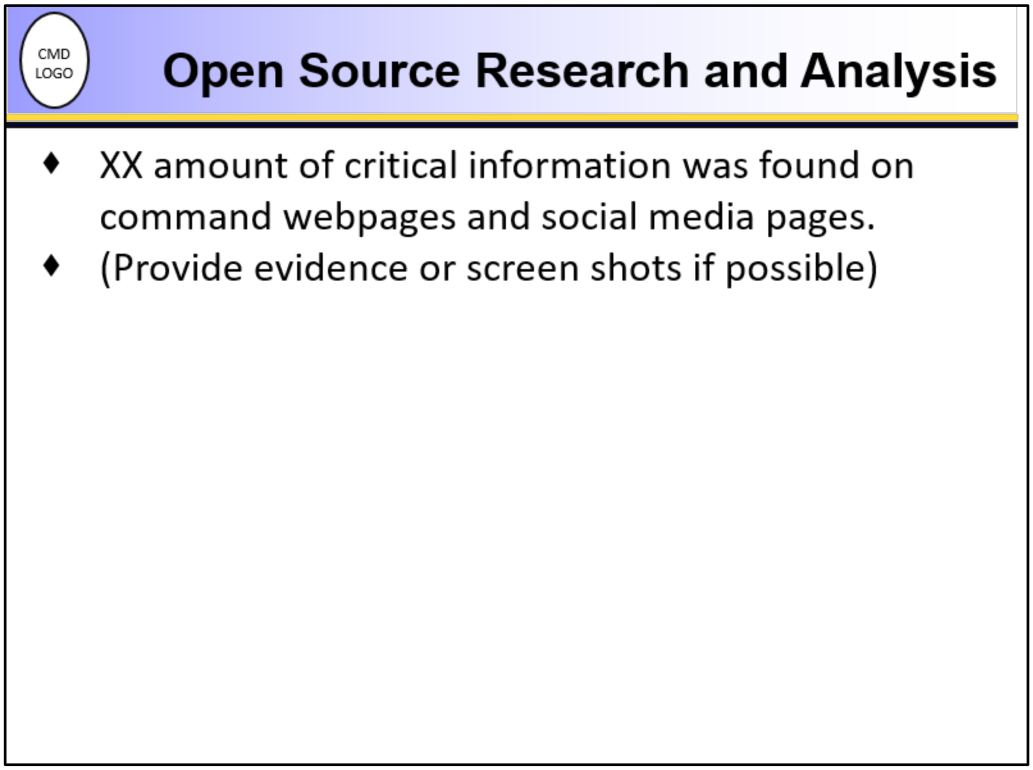


CMD LOGO

Bottom Line Up Front

- Bottom Line Up Front (BLUF)
- BLUF
- BLUF
- BLUF

Figure D-16. Example Operations Security Debrief: Bottom Line Up Front

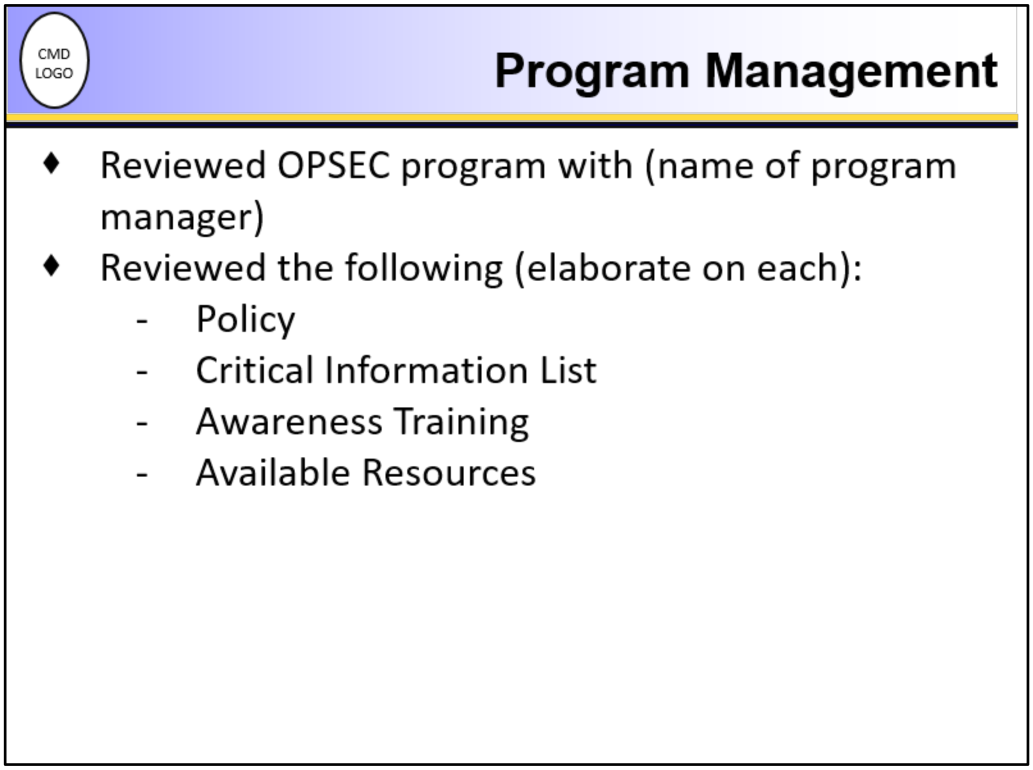


CMD LOGO

Open Source Research and Analysis

- XX amount of critical information was found on command webpages and social media pages.
- (Provide evidence or screen shots if possible)

Figure D-17. Example Operations Security Debrief: Open-source Research

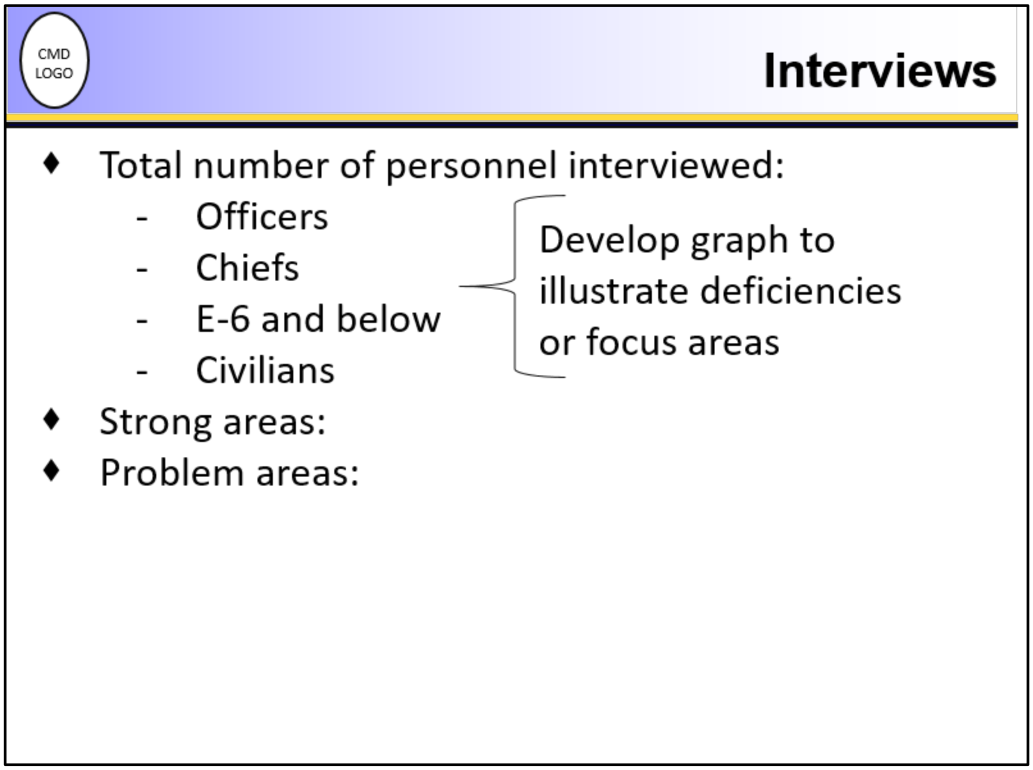


CMD LOGO

Program Management

- Reviewed OPSEC program with (name of program manager)
- Reviewed the following (elaborate on each):
  - Policy
  - Critical Information List
  - Awareness Training
  - Available Resources

Figure D-18. Example Operations Security Debrief: Program Management



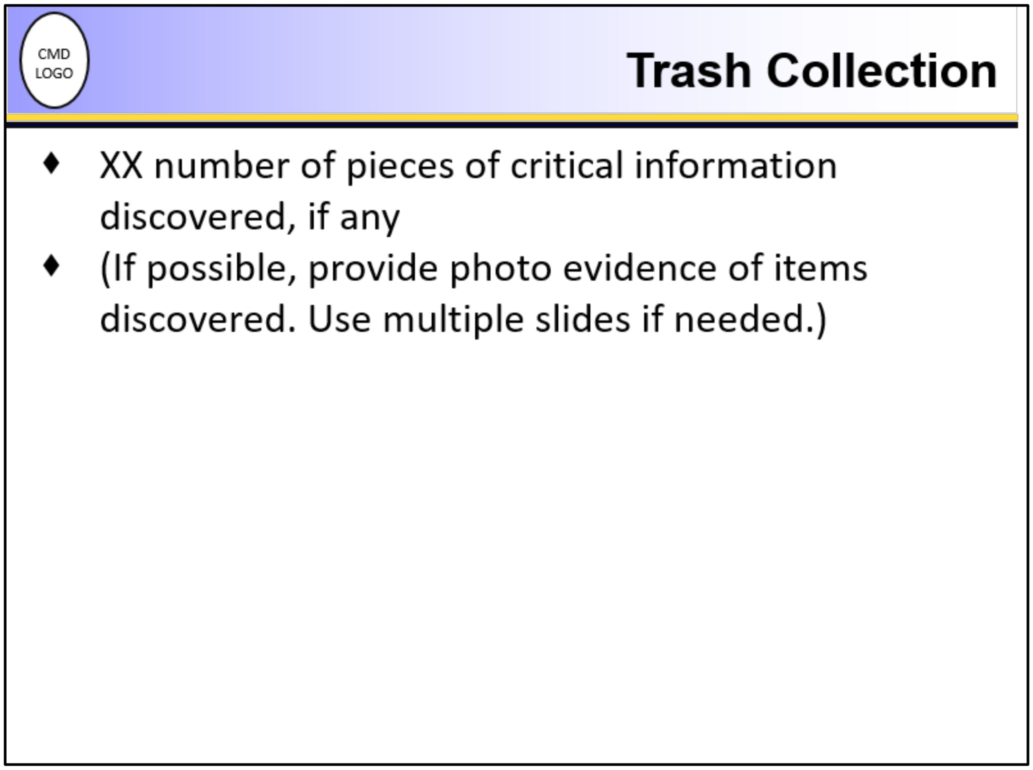
CMD LOGO

Interviews

- Total number of personnel interviewed:
  - Officers
  - Chiefs
  - E-6 and below
  - Civilians
- Strong areas:
- Problem areas:

Develop graph to illustrate deficiencies or focus areas

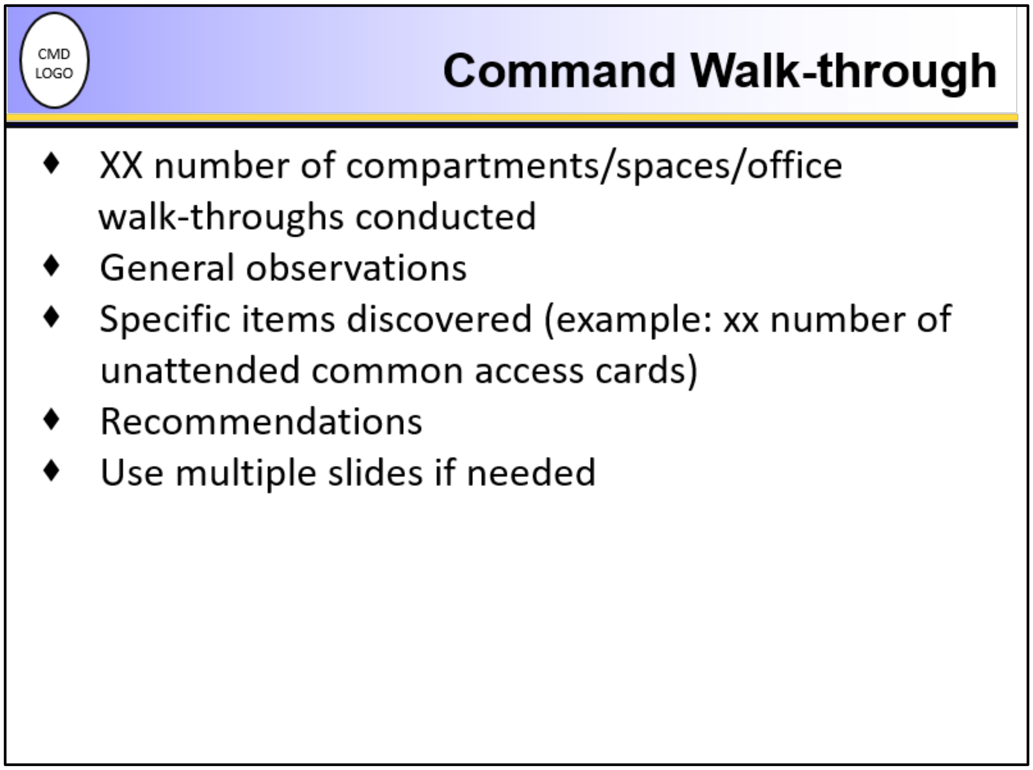
Figure D-19. Example Operations Security Debrief: Interviews



Trash Collection

- XX number of pieces of critical information discovered, if any
- (If possible, provide photo evidence of items discovered. Use multiple slides if needed.)

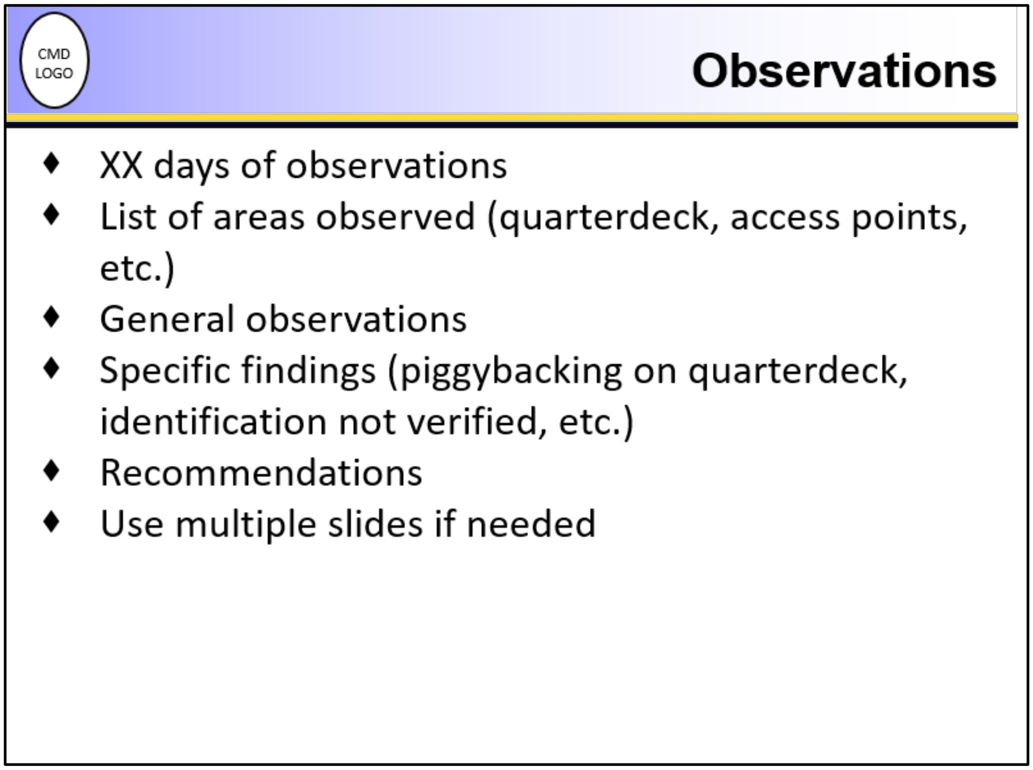
Figure D-20. Example Operations Security Debrief: Trash Collection



Command Walk-through

- XX number of compartments/spaces/office walk-throughs conducted
- General observations
- Specific items discovered (example: xx number of unattended common access cards)
- Recommendations
- Use multiple slides if needed

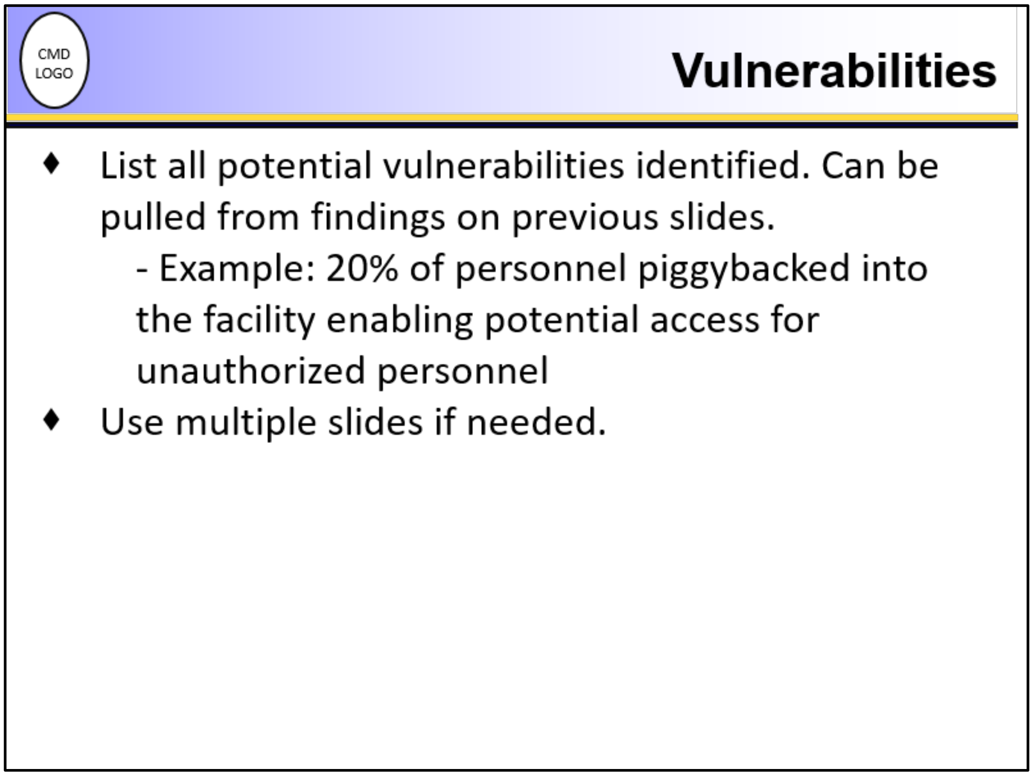
Figure D-21. Example Operations Security Debrief: Command Walk-through



Observations

- XX days of observations
- List of areas observed (quarterdeck, access points, etc.)
- General observations
- Specific findings (piggybacking on quarterdeck, identification not verified, etc.)
- Recommendations
- Use multiple slides if needed

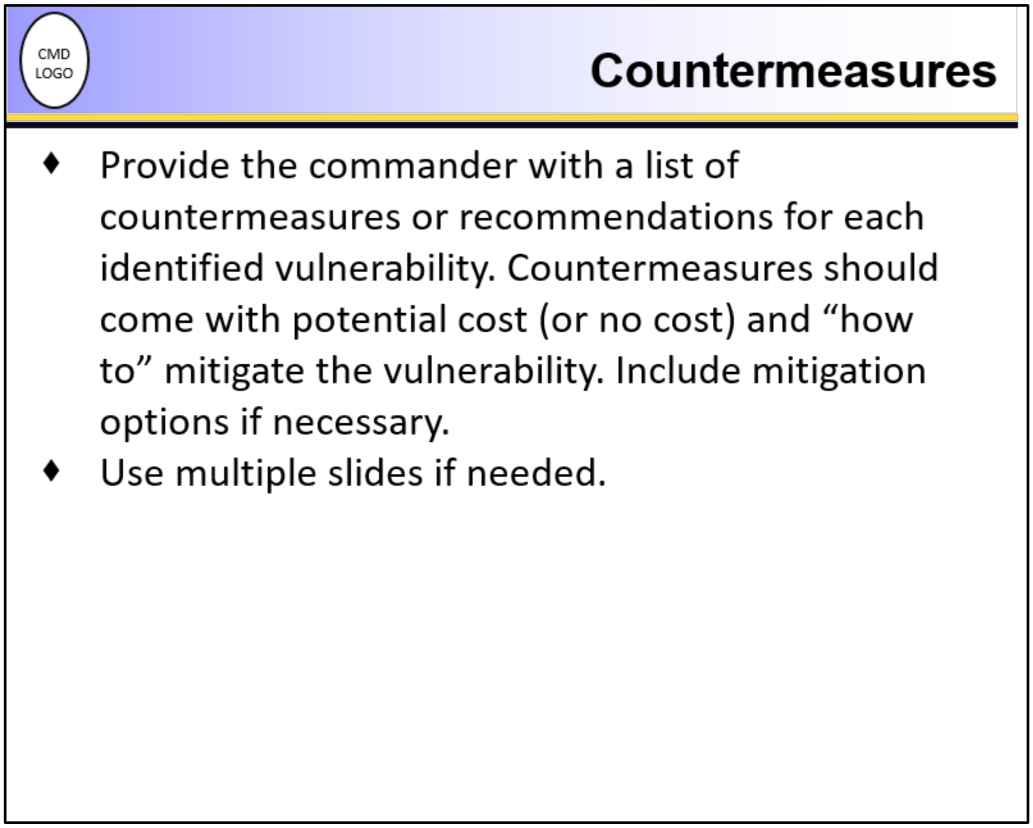
Figure D-22. Example Operations Security Debrief: Observations



Vulnerabilities

- List all potential vulnerabilities identified. Can be pulled from findings on previous slides.
  - Example: 20% of personnel piggybacked into the facility enabling potential access for unauthorized personnel
- Use multiple slides if needed.

Figure D-23. Example Operations Security Debrief: Vulnerabilities



Countermeasures

- Provide the commander with a list of countermeasures or recommendations for each identified vulnerability. Countermeasures should come with potential cost (or no cost) and “how to” mitigate the vulnerability. Include mitigation options if necessary.
- Use multiple slides if needed.

Figure D-24. Example Operations Security Debrief: Countermeasures

INTENTIONALLY BLANK

APPENDIX E

Operations Plan/Order Example

The following is an example Tab C (Operations Security) to Appendix 3 (Information Operations) to Annex C (Operations) of an operations plan/order.

Tab C—Operations Security.

1. (X) Situation. Refer to the operations annex and paragraphs in the base plan. When publishing the operations security (OPSEC) annex separately from the base order, it is necessary to copy the information here in detail. This allows the OPSEC annex to be a useful, stand-alone document. This section contains pertinent information from the intelligence preparation of the operations environment and the combined information overlay that informs OPSEC planning.

a. (X) Adversary Forces.

(1) (X) Current Adversary Intelligence Assessment. State the estimated adversary's assessment of friendly operations, capabilities, and intentions (i.e., what the adversary already understands of our friendly operational aspects). Figure E-1 is a planning template for friendly activities/critical information and indicator list worksheet.

(2) (X) Adversary Intelligence Capabilities. State the adversary's intelligence collection capabilities according to major categories (i.e., human intelligence, signals intelligence, open-source intelligence, geospatial intelligence, and measurement and signature intelligence). Address all potential sources, to include the capabilities of any non-belligerents who may provide support to the adversaries. Describe how the adversary's intelligence system works, to include the time required for intelligence to reach key decision makers. Identify major analytical organizations and key personalities. Discuss unofficial intelligence organizations, if any, that support the leadership. Identify strengths and weaknesses. Intelligence support organizations can provide conduit analysis on major adversary collection systems. Use Figure E-2.

b. (X) Friendly Forces.

(1) (X) Friendly Operations. Briefly describe the major actions and activities of friendly forces during execution of the base plan. Analyze the activities during friendly activity analysis and include the associated critical information, operational indicators, and operational profiles. Group activities by phase, if applicable. Use Figure E-1.

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

2. (X) Mission. Provide the OPSEC mission statement here.

3. (X) Execution.

a. (X) Concept of Operations. Place essential secrets and OPSEC tasks here. Describe the general concept to implement OPSEC events to achieve desired effects. Give general concept description by major activity, phases (if applicable), and how to integrate other information-related capabilities into the OPSEC plan. Address OPSEC support to other elements of the information operations plan, if applicable.

b. (X) Tasks. Identify specific OPSEC measures/countermeasures to implement by phase, if appropriate. Assign responsibility for execution to the command issuing the order or to subordinate commands. Add an exhibit to this tab for detailed or lengthy lists. See Figure E-3.

c. (X) Coordinating Instructions. Identify requirements to coordinate OPSEC measures/countermeasures between subordinate elements. Address required coordination with public affairs. Provide guidance on how to terminate OPSEC-related activities of this operation. Address declassification and public release of OPSEC-related information. Describe OPSEC assessments conducted in support of this plan. Identify any after action reporting requirements. See Figure E-4.

d. (X) Assessment. Describe the assessment concept. Monitor the effectiveness of OPSEC measures/countermeasures during execution. Identify specific intelligence requirements for assessments. Commanders and their staffs can use assessments to adjust ongoing activities and future OPSEC planning. Coordinate provisions for assessment with the command's intelligence and counterintelligence staffs to ensure requirements that support OPSEC receive the appropriate priority. Evaluate task accomplishment by assessing measures of effectiveness (MOEs) (Are we doing the right things to achieve the objective?) and measures of performance (MOPs) (Are things being done right?).

(1) (X) Identifying these items while the plan is in development and facilitate plan execution MOP (used to assess friendly accomplishment of tasks and mission execution) intelligence collection, MOEs indicators, and assessment of the OPSEC plan's effectiveness.

(2) (X) Identify specific MOPs. Provides a way to determine if OPSEC measures/countermeasures are being properly implemented. See Figure E-3.

(3) (X) Assess the OPSEC plan's MOE. Monitor the adversary's reaction to determine the measure's/countermeasures' effectiveness to achieve the objective. (Are desired effects achieved?) See Figure E-3.

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

f. (X) After Action Reports. Identify any requirements for after action reporting.

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

5. (X) Command and Control.

a. (X) Command Relationships.

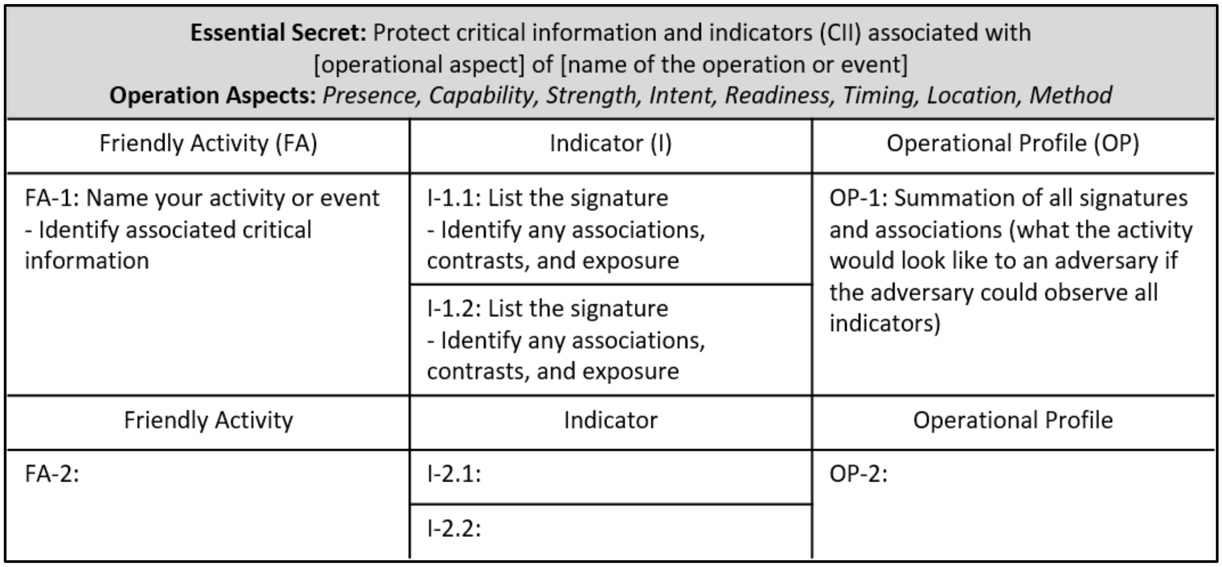
(1) (X) Approval. State approval authority for execution and termination.

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

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

b. (X) Command, Control, Communications, and Computer Systems. Address any special or unusual OPSEC-related communications system requirements. List all communications system-related OPSEC measures/countermeasures in 3.b.

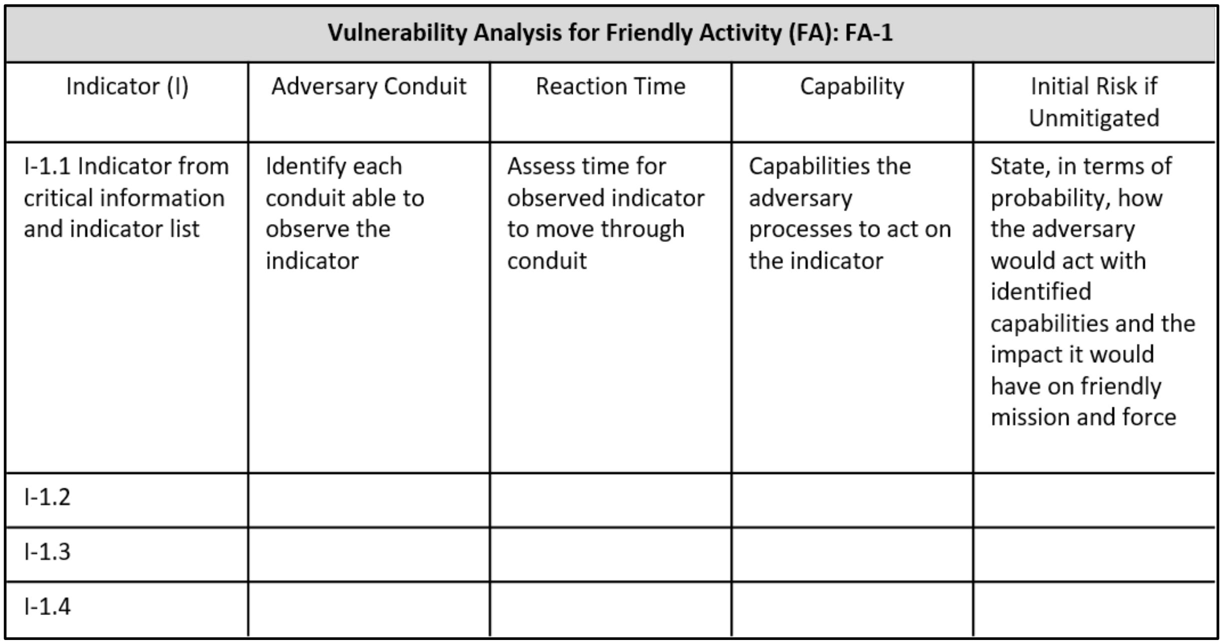
Exhibit (A).



Essential Secret: Protect critical information and indicators (CII) associated with [operational aspect] of [name of the operation or event] **Operation Aspects:** *Presence, Capability, Strength, Intent, Readiness, Timing, Location, Method*		
Friendly Activity (FA)	Indicator (I)	Operational Profile (OP)
FA-1: Name your activity or event - Identify associated critical information	I-1.1: List the signature - Identify any associations, contrasts, and exposure	OP-1: Summation of all signatures and associations (what the activity would look like to an adversary if the adversary could observe all indicators)
	I-1.2: List the signature - Identify any associations, contrasts, and exposure	
Friendly Activity	Indicator	Operational Profile
FA-2:	I-2.1:	OP-2:
	I-2.2:	

Figure E-1. Planning Template 1: Friendly Activity Worksheet

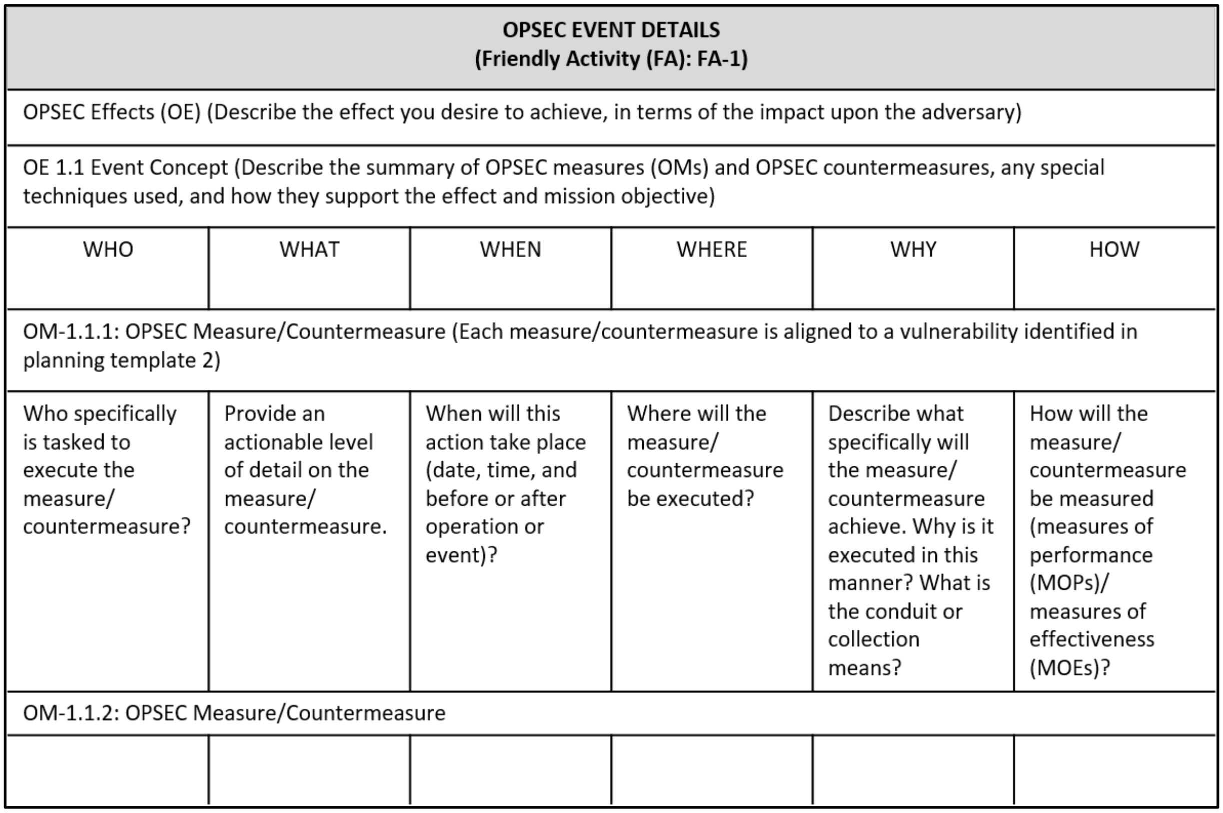
Exhibit (B).



Vulnerability Analysis for Friendly Activity (FA): FA-1				
Indicator (I)	Adversary Conduit	Reaction Time	Capability	Initial Risk if Unmitigated
I-1.1 Indicator from critical information and indicator list	Identify each conduit able to observe the indicator	Assess time for observed indicator to move through conduit	Capabilities the adversary processes to act on the indicator	State, in terms of probability, how the adversary would act with identified capabilities and the impact it would have on friendly mission and force
I-1.2				
I-1.3				
I-1.4				

Figure E-2. Planning Template 2: Vulnerability Worksheet

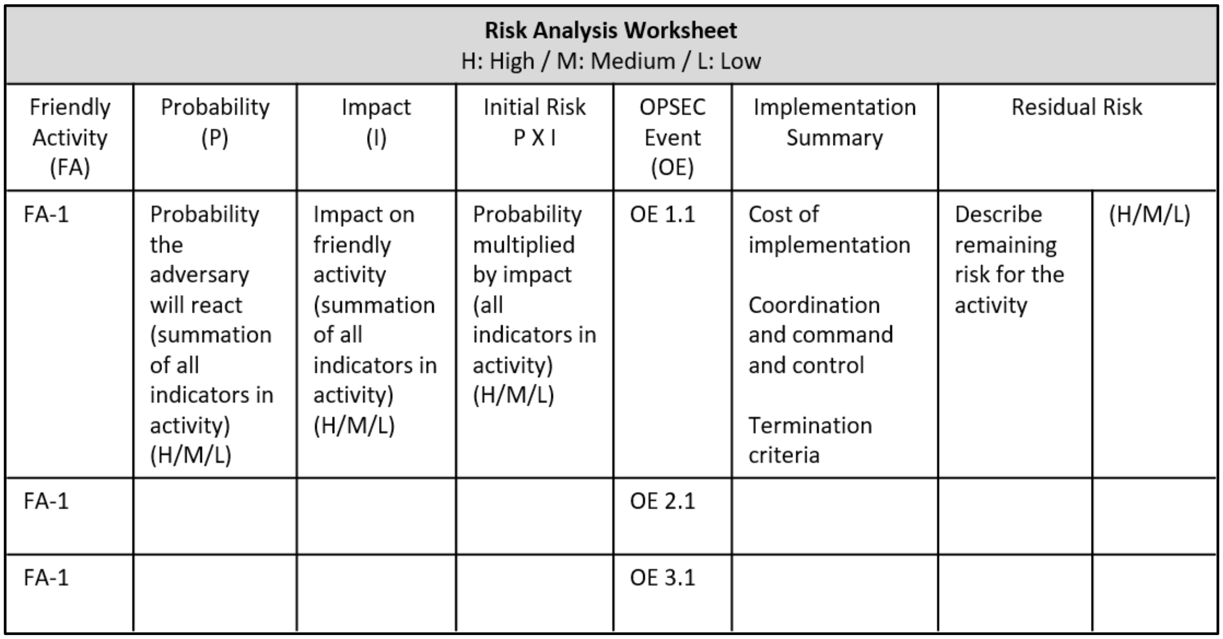
Exhibit (C).



OPSEC EVENT DETAILS **(Friendly Activity (FA): FA-1)**					
OPSEC Effects (OE) (Describe the effect you desire to achieve, in terms of the impact upon the adversary)					
OE 1.1 Event Concept (Describe the summary of OPSEC measures (OMs) and OPSEC countermeasures, any special techniques used, and how they support the effect and mission objective)					
WHO	WHAT	WHEN	WHERE	WHY	HOW
OM-1.1.1: OPSEC Measure/Countermeasure (Each measure/countermeasure is aligned to a vulnerability identified in planning template 2)					
Who specifically is tasked to execute the measure/ countermeasure?	Provide an actionable level of detail on the measure/ countermeasure.	When will this action take place (date, time, and before or after operation or event)?	Where will the measure/ countermeasure be executed?	Describe what specifically will the measure/ countermeasure achieve. Why is it executed in this manner? What is the conduit or collection means?	How will the measure/ countermeasure be measured (measures of performance (MOPs)/ measures of effectiveness (MOEs)?
OM-1.1.2: OPSEC Measure/Countermeasure					

Figure E-3. Planning Template 3: Operations Security Event Worksheet

Exhibit (D).



Risk Analysis Worksheet H: High / M: Medium / L: Low							
Friendly Activity (FA)	Probability (P)	Impact (I)	Initial Risk P X I	OPSEC Event (OE)	Implementation Summary	Residual Risk	
FA-1	Probability the adversary will react (summation of all indicators in activity) (H/M/L)	Impact on friendly activity (summation of all indicators in activity) (H/M/L)	Probability multiplied by impact (all indicators in activity) (H/M/L)	OE 1.1	Cost of implementation Coordination and command and control Termination criteria	Describe remaining risk for the activity	(H/M/L)
FA-1				OE 2.1			
FA-1				OE 3.1			

Figure E-4. Planning Template 4: Risk Analysis Worksheet

APPENDIX F

Command and Unit Movements

As U.S. naval forces deploy around the world conducting maritime operations, exercises, and dynamic force movements protecting critical information and preventing unauthorized disclosures is an extreme challenge.

Every Sailor must exercise vigilance while operating in the information environment and employ appropriate measures to protect the command's critical information and operations from disclosure.

Realize and understand that communication platforms like social media, hull and tail spotter enthusiasts, online search engines that pull and aggregate key words and terms from the internet, and inexpensive near–real-time imagery has made the effort to protect submarine and ship movements a daunting task. Organic sensors (e.g., automated information systems, radars, other navigation systems, and white shipping) combined with the open-source venues make the challenge seem impossible. Merely classifying information cannot guarantee the protection of operations.

The strongest protection available is the proper disclosure of both classified and critical information only to those individuals with appropriate clearance and a need to know.

The following information is generally not releasable unless declared otherwise by an on-scene commander, higher operational authority, or public affairs professionals with specific guidance to declassify the information and release it to the public:

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

2. Precise current location of forward-deployed units (i.e., latitude and longitude) and submarine movements, not including units while in port or submarines surfaced while transiting in/out of port.

3. Future plans or operations, rules of engagement, security measures, force protection, or deceptive actions used as part of an operation.

4. Information about downed aircraft or damaged ships while search and rescue operations are being planned or in progress, unless clearly in plain sight of shore or the media.

5. Intelligence collection activities (past and present), including intelligence methods, targets, and results.

The following are examples of unclassified information, some of which may be sensitive. Make the decision to release this information only after completing a risk assessment (using the five-step operations security (OPSEC) cycle) on the effects such a disclosure would have on the forces involved.

1. Disclosure of a specific date 48 hours in advance of arrival or departure of individual units to or from foreign ports or forward-deployed U.S. bases. While disclosure prior to this time may be necessary to support maintenance, logistics, and public affairs, keep these disclosures to the minimum required for coordination of unit arrival or departure.

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

Commanding officers must conduct OPSEC risk assessments prior to releasing critical information or following the inadvertent or malicious disclosure of critical information. Per SECNAVINST 3070.2A, Operations Security, punitive measures are authorized for individuals who willfully disclose unclassified, critical information. This includes sharing information with family members, who in turn post or share the same critical information online. Commanding officers conduct operational risk management assessments every day and shall do the same with OPSEC.

APPENDIX G
Acquisitions and Contracts

G.1 OVERVIEW

Consider operations security (OPSEC) throughout the lifecycle of the Department of Defense (DOD) acquisitions and contractor-supported efforts. It is essential to integrate OPSEC into the earliest stages, beginning with generating operational capabilities requirements and continuing through the award, design, development, test and evaluation, fielding, sustainment, and system disposal process. OPSEC requirements within acquisition and contracting ensure critical information and/or indicators are not prematurely released to vendors and the public. This applies to all types of contracts, including, but not limited to, service, support, acquisition, and fundamental research and grants. Contractors for defense systems acquisition programs and other types of DOD contracts will practice OPSEC to protect critical information and indicators, as specified in government contracts and subcontracts.

G.2 ORGANIZATIONAL RESPONSIBILITIES

Organizations requesting contract support determine and communicate the OPSEC measures required for each contract and ensure they are included in requests for proposal, statements of work, performance work statements (PWSs), statements of operations, or other contract documents. Organizations requesting contract support or originating contracts are responsible for the OPSEC review as they are the command most familiar with the critical information and contract requirements, especially for forward-deployed organizations. It is not the responsibility of the immediate superior in command (ISIC), nor the responsibility of the contracting specialists to conduct the OPSEC review. However, if the ISIC or contracting specialists question the contents of the contract, they are responsible for coordinating with the originator to ensure no disclosure of critical information occurs.

G.3 DOCUMENT REVIEWS

OPSEC officers or contracting specialists who attended a certified OPSEC officer course, in coordination with the contract requirement owners of the command, are responsible for reviewing contract documents to ensure critical information and indicators are withheld from the public. Use an approved critical information list (CIL) as a reference when conducting reviews. This emphasizes the importance of each command maintaining an accurate CIL and certified OPSEC officer.

If tasked with reviewing contacts for the command, assistant OPSEC officers, working group members, coordinators, and contract specialists are highly encouraged to attend formal OPSEC training. These members liaise with the OPSEC officer for technical guidance, as necessary, using the command approved CIL.

If it is determined that a contract document contains critical information and/or indicators associated with the performance of the contract, the requesting organization develops an OPSEC plan to protect the critical information and/or indicators associated with the contract throughout the lifecycle of the contract.

The requesting organization specifies the OPSEC requirements for contracts in requests for proposal, statements of work, PWSs, statements of operations, or other contract documents. Additionally, providing sufficient detail to ensure complete contractor understanding of the requirements to protect the critical information and/or indicators (e.g., what do you want the contractor to do, how do you want the contractor to comply, when do you want the contractor to comply, who is going to provide OPSEC training).

If required, organizations provide the contractor a copy of the OPSEC plan associated with the contract.

G.4 DOD CONTRACT SECURITY CLASSIFICATION SPECIFICATION FORM

DD 254, The Department of Defense Contract Security Classification Specification, for classified contracts may contain specific OPSEC measures to protect unclassified critical information. Even classified contracts that already have protective security measures in place, may still require additional OPSEC measures to protect the unclassified critical information. In this situation, check “Yes” in block 11.J of DD 254. In blocks 13 and/or 14 of DD 254, or on a separate document with specific direction, describe the OPSEC guidance or requirements.

G.4.1 Example of Contract Language

OPSEC guidance or language will vary depending on the stipulations or expectation of the services provided. Regardless, OPSEC must be included in contracts to protect critical information. Divulging critical information to the adversary can affect mission success and cause harm to military members, civilians, contractors, and their families. The following are categories and examples of OPSEC language used throughout the contract process.

G.4.2 Operations Security Background

- Background: OPSEC is a process used to protect unclassified critical information from exploitation by the adversary. Critical information or critical program information (CPI) is information that is not classified, but needs to be protected from unauthorized disclosure. Examples include information labeled controlled unclassified information (CUI), proprietary information, contractor critical information, limited distribution information, and personally identifiable information (PII).

- The contractor and all subcontractors shall provide OPSEC protection for critical information as identified in the CIL and CPI list, if applicable. The prime contractor and all subcontractors shall employ the OPSEC measures listed below to protect that information. Employ additional OPSEC measures as necessary. If provided with an OPSEC plan, the contractor and all subcontractors shall comply with that plan. These OPSEC requirements remain in effect throughout the life of the procurement, from award through the conclusion of services at the end of the period of performance or other procurement termination. If required, the contractor and all subcontractors shall prepare an OPSEC plan.

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

G.4.3 Minimum Protection Requirements for Critical Information

- Critical information is exempt from public release under Exemption 2 of Title 32 U.S.C. § 552, Freedom of Information Act. It is designated CUI. Specific CPI, for reasons of OPSEC is not identified to solicitors prior to award. CPI will be identified to the successful solicitor only after receipt of contract award.

G.4.4 Controlled Unclassified Information

- CUI is official information that requires the application of controls and protective measures for a variety of reasons and not approved for public release, to include technical information, proprietary data, information requiring protection under Title 5 U.S.C. § 552a, Privacy Act of 1974, and government-developed privileged information involving the award of contracts. CUI is a categorical designation that refers to unclassified information that does not meet the standards for national security classification under executive order(s), but is pertinent to the national interest of the United States or to the important interests of entities outside the Federal Government, and under law or policy requires protection from unauthorized disclosure, special handling safeguards, or prescribed limits on exchange or dissemination.

- Minimum requirements for access to CUI. Prior to access, contractor personnel requiring access to Department of Navy (DON) CUI or "user-level access to DON or DOD networks and information systems, system security, and network defense systems, or to system resources providing visual access and/or ability to input, delete, or otherwise manipulate critical information without controls to identify and deny critical information," who do not have clearance eligibility are required to submit an SF 85P, Questionnaire for Public Trust Positions, through the cognizant facility security officer (FSO) or contractor entity representative for a suitability determination by DON Central Adjudication Facility.

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

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

- All UNCLASSIFIED documents created under this contract that contain CUI information will be marked "CONTROLLED UNCLASSIFIED INFORMATION" on the bottom of the cover page and interior pages.

- Classified documents containing CUI do not require any markings on the cover of the document. However, the interior pages containing only CUI shall be marked at the top and bottom center with "CONTROLLED UNCLASSIFIED INFORMATION." Only unclassified portions containing CUI shall be marked with "(CUI)" immediately before each unclassified CUI portion.

- Mark all CUI released to the contractor with the following statement prior to transfer: THIS DOCUMENT CONTAINS INFORMATION EXEMPT FROM MANDATORY DISCLOSURE UNDER THE FOIA. EXEMPTIONS(S) _______ APPLY.

- The originator or other competent authority can remove the CUI marking. The contractor shall not remove any CUI marking without written authorization from the author. The Government notifies the contractor when termination of the CUI status occurs.

- With authorization, the contractor can disseminate CUI to its employees and those having a need to know the information to accomplish the requirements of the contract.

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

- Deliver CUI information via United States Postal Service first-class mail, parcel post, and fourth-class mail for bulk shipments only. The contractor shall not permit CUI to enter foreign postal systems and parcel delivery systems.

- When no longer needed, return CUI information to appropriate Government custody or destroy in a manner precluding reconstruction of the information.

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

- The FSO provides any necessary access briefings required for contract performance (e.g., North Atlantic Treaty Organization and others).

- Classified information performance occurs only at locations specified on the DD 254.

G.4.5 Personally Identifiable Information

- Protect PII in accordance with DOD and Navy directives, and in such a manner as to prevent unauthorized disclosure. Encrypt or password protect emails containing PII.

G.4.6 Operations Security Measures

- The contractor shall protect all critical information in a manner appropriate to the nature of the information, including the use of the necessary countermeasures, as listed below, applicable to specific items:

1. Encrypt and password protect electronically stored critical information.

2. Encrypt or password protect email containing critical information.

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

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

5. Properly mark critical information with warnings, to include at a minimum "CONTROLLED UNCLASSIFIED INFORMATION." As appropriate to the nature of the critical information, it shall also be marked with "UNCLASSIFIED BUT SENSITIVE," "PRIVACY ACT INFORMATION," "PERSONALLY IDENTIFYING INFORMATION," "PROTECT FROM UNAUTHORIZED DISCLOSURE," or other similar statements cautioning protection of the critical information.

6. Restrict disclosure of critical information at meetings and conferences, including teleconferences, to the minimum number of participants necessary to accomplish the performance requirement.

7. Immediately and appropriately destroy all critical information in a manner precluding reconstruction no longer needed under this requirement.

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

9. Maintain current and completed Navy-mandated information assurance (IA) and OPSEC training by all personnel handling critical information.

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

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

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

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

14. Limit the inclusion of critical information in contract and budget documents, presentations, press releases, and other publications to those essential to the performance of this requirement.

15. Use protected databases, strong passwords, and the protection of user identifications.

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

G.4.7 Compromise

- The contractor shall notify the SME, FSO, and security office immediately of all known and suspected compromises of critical information, classified information, or PII. If the SME is unreachable, the contractor shall notify the contracting officer (or the command duty officer if after normal work hours).

G.4.8 Additional Contract Language for Operations Security Requirements

- Consider including the following Defense Federal Acquisition Regulation Supplement (DFARS) clauses for all service support contracts: DFARS 252.227-7020, DFARS 252.204.7000, DFARS 252.204.7003, DFARS 252.204.7008, DFARS 252.204.7009, DFARS 252.204.7012.

G.4.9 Government Furnished Training

- The Government provides contractors access to all mandated IA and cyberspace awareness training required in support of this contract to allow establishment of government information technology user accounts and access to government operated networks. All other training requirements required to attain or maintain skill levels and qualifications of contractor personnel are considered contractor responsibility and will not be reimbursed by the Government.

G.4.10 Security Requirements

- Do not grant access to personnel without the appropriate clearance to designated government facilities. In accordance with these requirements, those personnel cannot perform work in support of this PWS. Detailed security requirements shall be in accordance with DD 254.

- The contractor and its employees shall not divulge any information about files, data, processing activities or functions, user identification, passwords, or other knowledge to anyone who does not have authorization for access to such information. Such conduct may be cause for criminal prosecution and imposition of severe criminal and civil penalties.

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

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

- The contractor ensures employees comply with established command OPSEC policy to protect the Government's critical information, in accordance with SECNAVINST 3070.20A, Operations Security. New contractor employees are required to complete welcome aboard training and all contractor employees must complete annual OPSEC awareness training. All contractor employees shall complete IA, cyberspace awareness, and OPSEC training before issuance of network access and conduct training annually thereafter.

G.4.11 Loss or Suspension of Security Facility Clearance

- The Government reserves the right to direct the removal of a contractor from work, directly or indirectly, whenever there is probable cause to warrant such action in the interest of national security. This action can be taken whether or not there is sufficient cause to warrant terminating the contractor's facility clearance or employee's security clearance. The Government also reserves the right to remove any contractor to investigate allegations of misconduct that may jeopardize the security of the project in the opinion of the contracting officer.

G.4.12 Public Release Statement

- Any information (classified and unclassified) pertaining to this contract shall not be released for public dissemination except as provided by DoD Manual 5220.32, Volume 1, National Industrial Security Program: Industrial Security Procedures For Government Activities, or unless it has been approved for public release by an appropriate U.S. Government authority. Submit public release proposals for approval at least 10 working days (or as directed by the hiring activity) prior to desired release/disclosure. Non-DOD user agencies submit requests for disclosure at least 15 working days prior to requested release date.

G.5 SERVICE REQUIREMENTS REVIEW BOARD

The service requirements review board (SRRB) is a DOD mandated contract review process. The objective is to ensure requirements seeking approval for acquisition are compliant with regulation, policy, and guidance; mitigate duplicative requirements; identify unneeded or low priority requirements that can be reduced or eliminated, allowing savings transfer to higher priority objectives; and acquire services in the most efficient and effective manner possible. Institute the OPSEC review for contracts within the SRRB process. Figure G-1 illustrates the SRRB process. The SRRB process is tailorable to specific fleet processes.

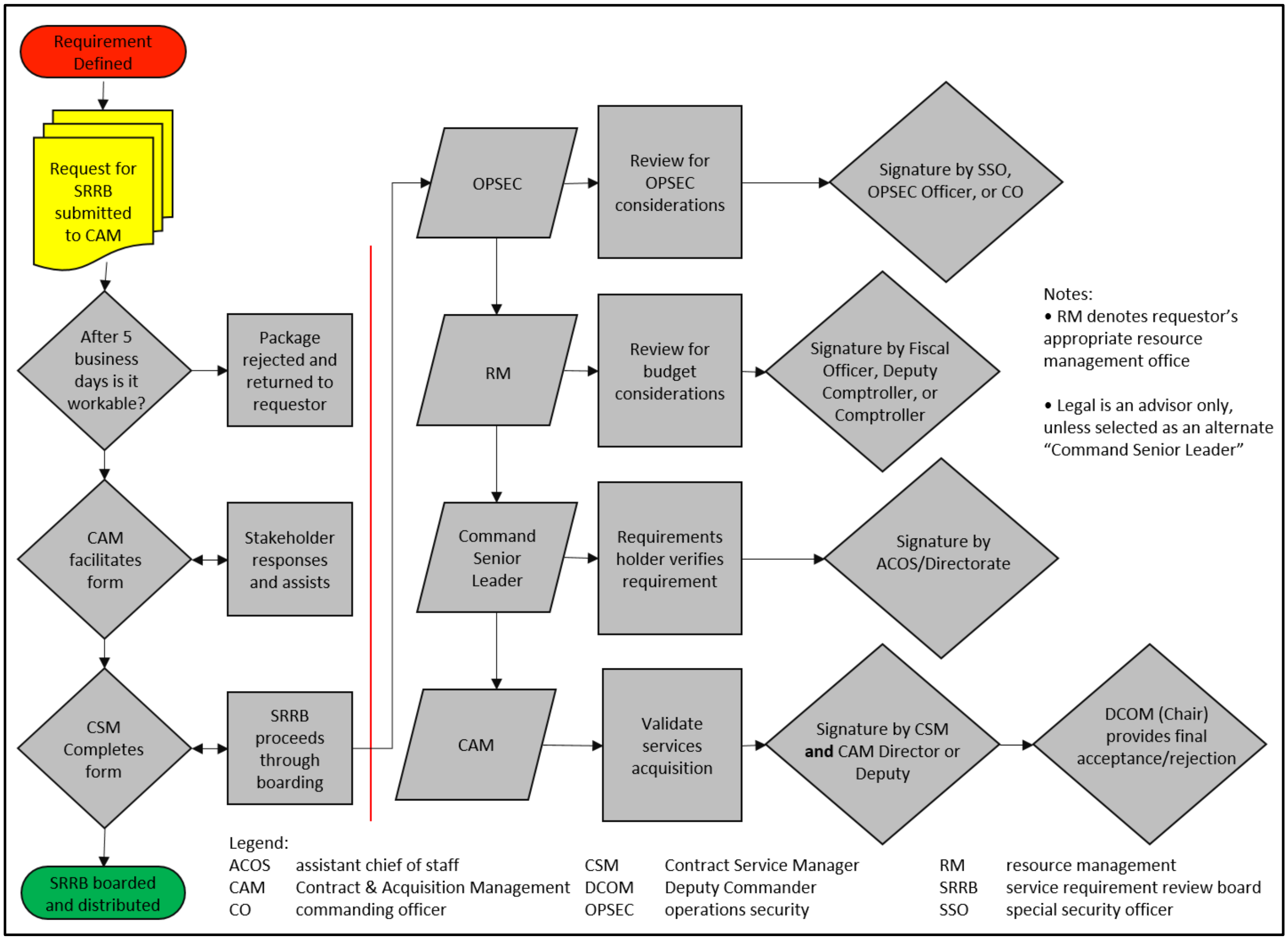
G.6 GOVERNING INSTRUCTIONS

The following publications provide additional policy and instructions concerning the acquisition and contract process:

1. DODI 5000.74, Defense Acquisition of Services

2. FAR, Volume I-Parts 1 to 51 (https://www.acquisition.gov)

3. COMUSFLTFORCOMINST 4200.3A, Service Requirements Review Board.


Requirement Defined
Request for SRRB submitted to CAM
After 5 business days is it workable?
Package rejected and returned to requestor
CAM facilitates form
Stakeholder responses and assists
CSM Completes form
SRRB proceeds through boarding
SRRB boarded and distributed
OPSEC
Review for OPSEC considerations
Signature by SSO, OPSEC Officer, or CO
RM
Review for budget considerations
Signature by Fiscal Officer, Deputy Comptroller, or Comptroller
Command Senior Leader
Requirements holder verifies requirement
Signature by ACOS/Directorate
CAM
Validate services acquisition
Signature by CSM **and** CAM Director or Deputy
DCOM (Chair) provides final acceptance/rejection

Notes:

- RM denotes requestor's appropriate resource management office
- Legal is an advisor only, unless selected as an alternate "Command Senior Leader"

Legend:

ACOS	assistant chief of staff	CSM	Contract Service Manager	RM	resource management
CAM	Contract & Acquisition Management	DCOM	Deputy Commander	SRRB	service requirement review board
CO	commanding officer	OPSEC	operations security	SSO	special security officer

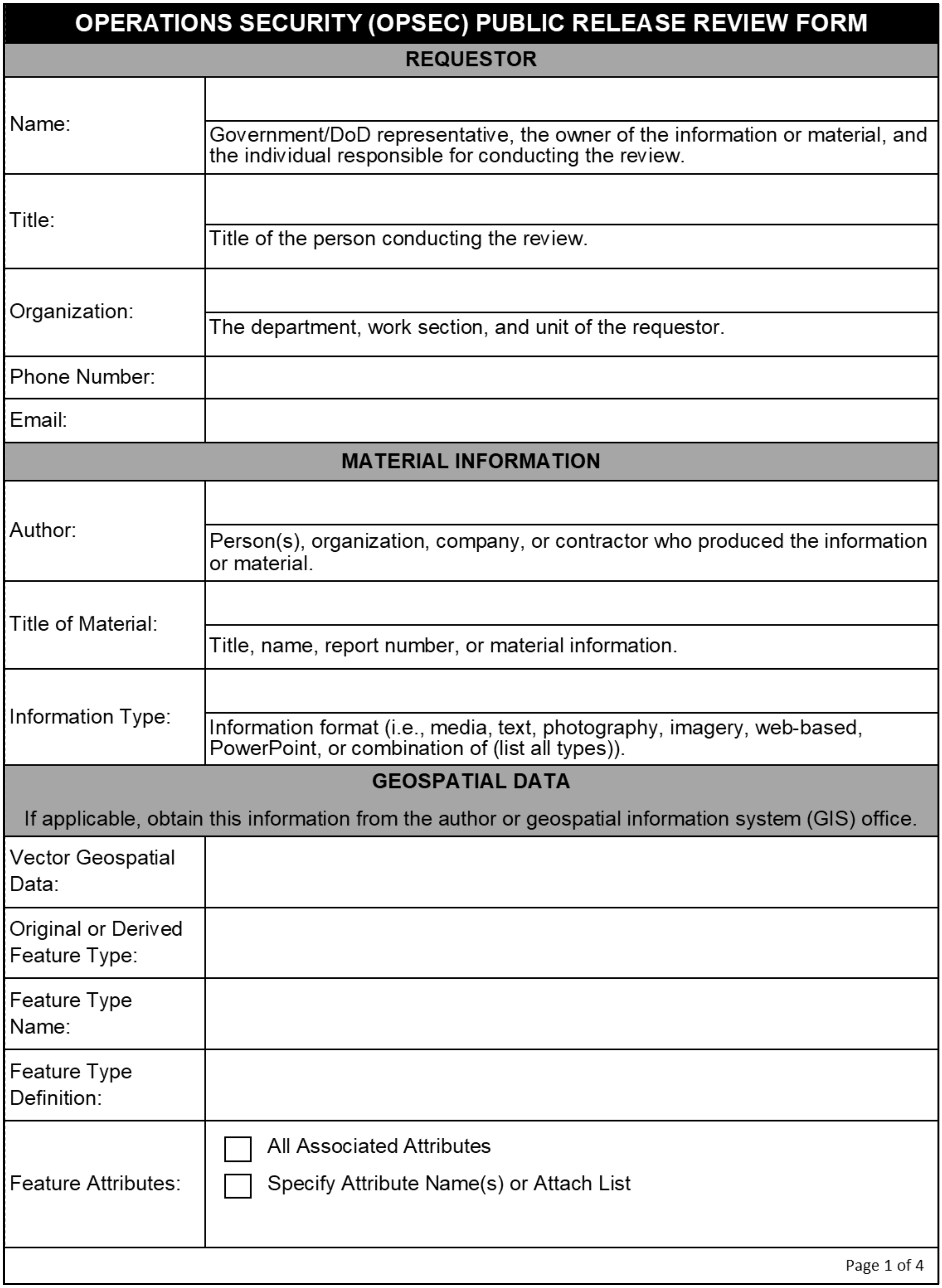
Figure G-1. Sample Service Requirements Review Board Process

INTENTIONALLY BLANK

APPENDIX H

Operations Security Public Release Review

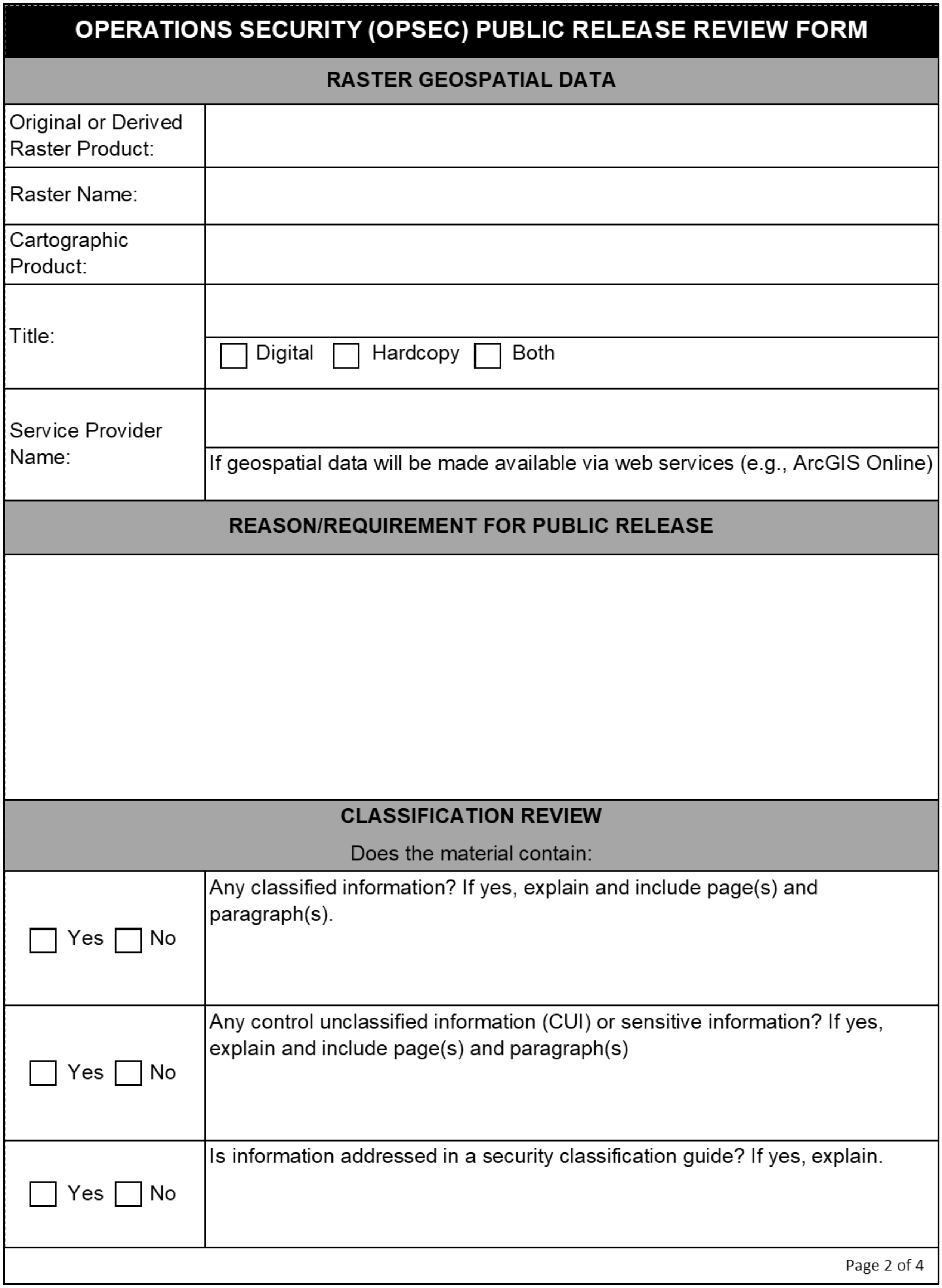
In accordance with SECNAVINST 3070.2A, Operations Security, all commands must utilize a process to review information prior to release into the public domain. Use the operations security (OPSEC) public release form (see Figure H-1) and decision flow chart (see Figure H-2) as tools or processes to review information for public release. Tailor the form and flow chart to fit the command's review requirements. In the event that your command has already developed a review process, there is no need to utilize the form.



OPERATIONS SECURITY (OPSEC) PUBLIC RELEASE REVIEW FORM

REQUESTOR	
Name:	 Government/DoD representative, the owner of the information or material, and the individual responsible for conducting the review.
Title:	 Title of the person conducting the review.
Organization:	 The department, work section, and unit of the requestor.
Phone Number:	
Email:	
MATERIAL INFORMATION	
Author:	 Person(s), organization, company, or contractor who produced the information or material.
Title of Material:	 Title, name, report number, or material information.
Information Type:	 Information format (i.e., media, text, photography, imagery, web-based, PowerPoint, or combination of (list all types)).
GEOSPATIAL DATA If applicable, obtain this information from the author or geospatial information system (GIS) office.	
Vector Geospatial Data:	
Original or Derived Feature Type:	
Feature Type Name:	
Feature Type Definition:	
Feature Attributes:	□ All Associated Attributes □ Specify Attribute Name(s) or Attach List
	Page 1 of 4

Figure H-1. Operations Security Public Release Review Form (Sheet 1 of 4)



OPERATIONS SECURITY (OPSEC) PUBLIC RELEASE REVIEW FORM

RASTER GEOSPATIAL DATA

Original or Derived Raster Product:	
Raster Name:	
Cartographic Product:	
Title:	
	□ Digital □ Hardcopy □ Both
Service Provider Name:	
	If geospatial data will be made available via web services (e.g., ArcGIS Online)

REASON/REQUIREMENT FOR PUBLIC RELEASE

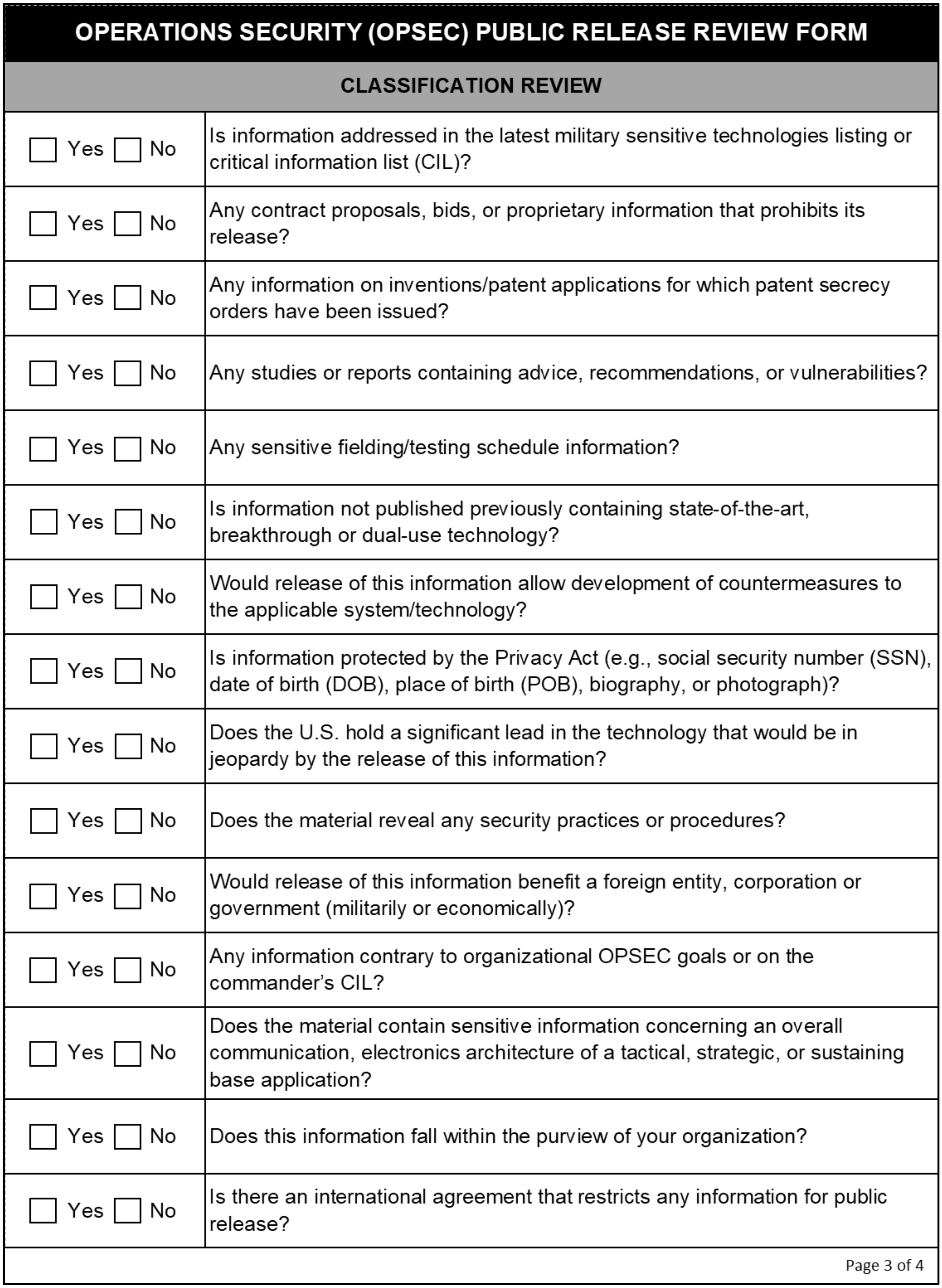
CLASSIFICATION REVIEW

Does the material contain:

□ Yes □ No	Any classified information? If yes, explain and include page(s) and paragraph(s).
□ Yes □ No	Any control unclassified information (CUI) or sensitive information? If yes, explain and include page(s) and paragraph(s)
□ Yes □ No	Is information addressed in a security classification guide? If yes, explain.

Page 2 of 4

Figure H-1. Operations Security Public Release Review Form (Sheet 2 of 4)



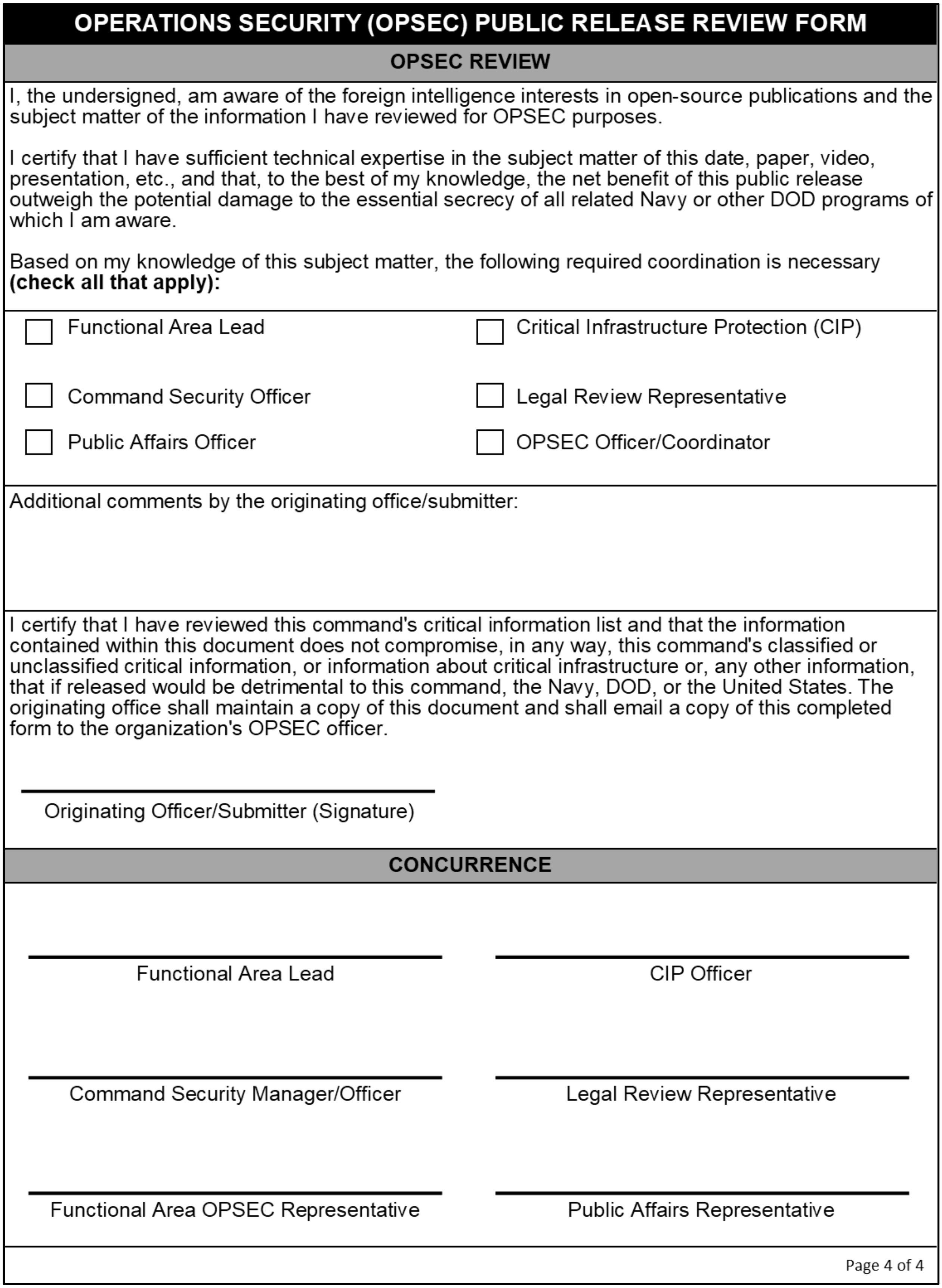
OPERATIONS SECURITY (OPSEC) PUBLIC RELEASE REVIEW FORM

CLASSIFICATION REVIEW

□ Yes □ No	Is information addressed in the latest military sensitive technologies listing or critical information list (CIL)?
□ Yes □ No	Any contract proposals, bids, or proprietary information that prohibits its release?
□ Yes □ No	Any information on inventions/patent applications for which patent secrecy orders have been issued?
□ Yes □ No	Any studies or reports containing advice, recommendations, or vulnerabilities?
□ Yes □ No	Any sensitive fielding/testing schedule information?
□ Yes □ No	Is information not published previously containing state-of-the-art, breakthrough or dual-use technology?
□ Yes □ No	Would release of this information allow development of countermeasures to the applicable system/technology?
□ Yes □ No	Is information protected by the Privacy Act (e.g., social security number (SSN), date of birth (DOB), place of birth (POB), biography, or photograph)?
□ Yes □ No	Does the U.S. hold a significant lead in the technology that would be in jeopardy by the release of this information?
□ Yes □ No	Does the material reveal any security practices or procedures?
□ Yes □ No	Would release of this information benefit a foreign entity, corporation or government (militarily or economically)?
□ Yes □ No	Any information contrary to organizational OPSEC goals or on the commander's CIL?
□ Yes □ No	Does the material contain sensitive information concerning an overall communication, electronics architecture of a tactical, strategic, or sustaining base application?
□ Yes □ No	Does this information fall within the purview of your organization?
□ Yes □ No	Is there an international agreement that restricts any information for public release?

Page 3 of 4

Figure H-1. Operations Security Public Release Review Form (Sheet 3 of 4)



OPERATIONS SECURITY (OPSEC) PUBLIC RELEASE REVIEW FORM

OPSEC REVIEW

I, the undersigned, am aware of the foreign intelligence interests in open-source publications and the subject matter of the information I have reviewed for OPSEC purposes.

I certify that I have sufficient technical expertise in the subject matter of this date, paper, video, presentation, etc., and that, to the best of my knowledge, the net benefit of this public release outweigh the potential damage to the essential secrecy of all related Navy or other DOD programs of which I am aware.

Based on my knowledge of this subject matter, the following required coordination is necessary **(check all that apply):**

□ Functional Area Lead

□ Command Security Officer

□ Public Affairs Officer

□ Critical Infrastructure Protection (CIP)

□ Legal Review Representative

□ OPSEC Officer/Coordinator

Additional comments by the originating office/submitter:

I certify that I have reviewed this command's critical information list and that the information contained within this document does not compromise, in any way, this command's classified or unclassified critical information, or information about critical infrastructure or, any other information, that if released would be detrimental to this command, the Navy, DOD, or the United States. The originating office shall maintain a copy of this document and shall email a copy of this completed form to the organization's OPSEC officer.

Originating Officer/Submitter (Signature)

CONCURRENCE

Functional Area Lead

CIP Officer

Command Security Manager/Officer

Legal Review Representative

Functional Area OPSEC Representative

Public Affairs Representative

Page 4 of 4

Figure H-1. Operations Security Public Release Review Form (Sheet 4 of 4)

Decision Flowchart 'Section by Section' Guide

Article topic on the command's critical information list (CIL)?

The command's CIL is based on current threats to, and adversaries interests in, various existing or emerging U.S. technologies or capabilities.

Is the information public knowledge/widely known?

To your knowledge, is all the information in the article widely known within your professional community? Is the fact that the command has efforts or capabilities in this area publically known? ***Both*** must be 'yes' to follow the "Yes" path.

Is the overall level of detail correct for the topic *and* necessary?

Ensure you consider the volume of and level of detail of information in the article as a whole. If it's more than is really necessary to make the points of the article, reword with less detail.

Is the information needed to 'kill, counter, or clone' a program or system?

To your knowledge, is there information in the article that could reasonably be expected to, or used to, kill, counter, or clone the effort or capability by an adversary or competitor?

Consideration must be given to necessity to publish article, seek OPSEC guidance.

If the information in the article is on the command's CIL, it is of value to an adversary. This list is based on the threat to U.S. technologies or capabilities, coupled with potential adversary interest in them. Therefore, consideration must be given as to the prudence of publishing information on the topic, or to the amount of information provided. Articles that fall in this category must be given an OPSEC review prior to any public release.

Seek OPSEC guidance for assistance with article revision.

Contact the Command OPSEC manager for assistance in rewording the article to better consider OPSEC.

No significant OPSEC concerns, article could be published as written.

The article's information and level of detail should, after this thorough review, have no OPSEC concerns. An author can always still seek additional OPSEC guidance, if desired.

Figure H-2. Operations Security Decision Flowchart (Sheet 1 of 2)

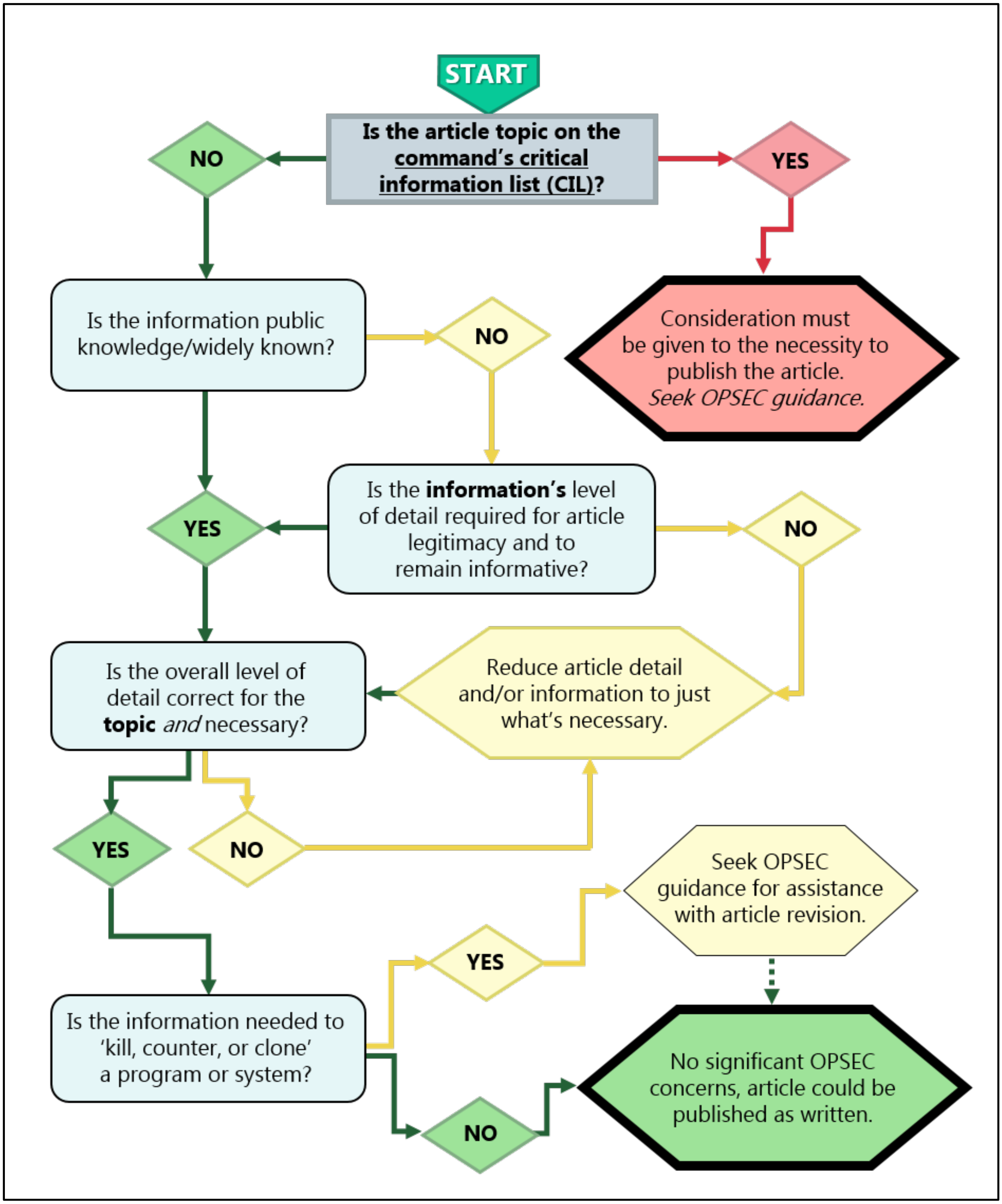

START
Is the article topic on the command's critical information list (CIL)?
NO
YES
Is the information public knowledge/widely known?
NO
Consideration must be given to the necessity to publish the article. Seek OPSEC guidance.
YES
Is the information's level of detail required for article legitimacy and to remain informative?
NO
Is the overall level of detail correct for the topic and necessary?
Reduce article detail and/or information to just what's necessary.
YES
NO
Seek OPSEC guidance for assistance with article revision.
YES
Is the information needed to 'kill, counter, or clone' a program or system?
No significant OPSEC concerns, article could be published as written.
NO

Figure H-2. Operations Security Decision Flowchart (Sheet 2 of 2)

INTENTIONALLY BLANK

REFERENCES

NWP 5-01 (MAY 2021), Navy Planning

NTRP 1-01 (JUN 2021), The Navy Warfare Library User Manual

NTRP 1-02 (OCT 2022), Navy Supplement to the DOD Dictionary of Military and Associated Terms

OPNAVINST 2201.3C (MAY 2020), Communications Security Monitoring of Navy Telecommunications and Information Technology Systems

SECNAVINST 3070.20A (MAY 2019), Operations Security

COMUSFLTFORCOMINST 4200.3A (JAN 2019), Service Requirements Review Board

JP 3-0 (JUN 2022), Joint Campaigns and Operations

JP 3-13.3 (JAN 2016), Operations Security

AFI 10-701 (JUN 2020), Operations Security

DD 2056, Telephone Monitoring Notification Decal, https://www.dami.army.pentagon.mil/site/sso/docs/InfoSec/DD%20Form%202056.pdf

DD 254, The Department of Defense Contract Security Classification Specification

DODD 3115.18 (AUG 2020), DOD Access to and Use of Publicly Available Information

DODI 5000.74 (JUN 2021), Defense Acquisition of Services

DODM 5205.02 (OCT 2020), DOD Operations Security Program Manual

DODM 5220.32, Volume 1, National Industrial Security Program: Industrial Security Procedures For Government Activities

DFARS 252.204.7000, Non-Estoppel

DFARS 252.204.7003, Termination

DFARS 252.204.7008, Computation of Royalties

DFARS 252.204.7009, Reporting and Payment of Royalties

DFARS 252.204.7012, Patent License and Release Contract

DFARS 252.227-7020, Rights in Special Works

FAR Volume I-Parts 1 to 51 (2019), https://www.acquisition.gov

Joint Forces Staff College Defense Operations Security Planners Course Handbook

NSDD 298 (JAN 1988), National Operations Security Program

NTISSD 600 (APR 1990), Communications Security Monitoring

SF 85P, Questionnaire for Public Trust Positions

Title 32 U.S.C. § 552 (2016), Freedom of Information Act

Title 5 U.S.C. § 552a (2020), Privacy Act of 1974

Center for Cryptologic History, PURPLE DRAGON: The Origin and Development of the United States OPSEC Program, series VI volume 2, 1993, https://www.nsa.gov/portals/75/documents/news-features/declassified-documents/cryptologic-histories/purple_dragon.pdf

Hern, Alex, Fitness tracking app Strava gives away location of secret US army bases, The Guardian, January 28, 2018, https://www.theguardian.com/world/2018/jan/28/fitness-tracking-app-gives-away-location-of-secret-us-army-bases

Smith, Maggie & Stark, Nick, Open-source Data is Everywhere—Except the Army's Concept of Information Advantage, Modern War Institute at West Point, May 24, 2022, https://mwi.usma.edu/open-source-data-is-everywhere-except-the-armys-concept-of-information-advantage/

Enterprise Protection Risk Management, http://eprmhelp.countermeasures.com/

United States Navy Home Page, www.navy.mil

United States Navy Operations Security Support Team, https://www.navifor.usff.navy.mil/opsec

SUGGESTED READING

NTRP 1-03.1 (DEC 2020), Operational Reports

OPNAVINST 4400.11A (JUN 2020), Husbanding Service Provider Program Policy

GLOSSARY

administrative indicator. Unique documents or other observable coordination normally attributed to a friendly activity or capability employment. (JFSC DOPC)

adversary. A party acknowledged as potentially hostile to a friendly party and against which the use of force may be envisaged. (JP 3-0)

conditioning. An operations security technique involving the introduction and repetition of an operational pattern to generate a sense of normalcy to the observer. Conditioning is normally done to create an opportunity for surprise or to induce a contrast creating a friendly advantage. (JFSC DOPC)

conduit. A pathway over which data or information is collected, passed, analyzed and delivered to decision makers. A typical conduit consists of a sensor, links for the transmission of data or information, and nodes through which data passes. (AFI 10-701)

critical information. Specific facts about friendly intentions, capabilities, and activities needed by adversaries for them to plan and act effectively so as to guarantee failure or unacceptable consequences for friendly mission accomplishment. (SECNAV 3070.2A)

critical information and indicator list. A list of critical information and indicators for a specific command or organization. (SECNAV 3070.2A)

critical information list. A list of critical information that has been fully coordinated within an organization and approved by the senior decision maker, and is used by all personnel in the organization to identify unclassified information requiring application of OPSEC measures. (DODM 5205.02)

dazzling. An operations security technique that attempts to confuse the adversary by creating multiple contrasts in other concurrent friendly activities to draw attention away from critical information and indicators that cannot be fully concealed or protected. (JFSC DOPC)

deception in support of operations security. A military deception activity that protects friendly operations, personnel, programs, equipment, and other assets against foreign intelligence entity collection. (NTRP 1-02)

essential secrecy. The condition achieved from the denial of critical information and indicators to adversaries through the combined efforts of the OPSEC program and traditional security programs. (SECNAV 3070.2A)

essential secret. Specific aspects of planned friendly operations that, if compromised, would lead to adversary identification of exploitable conditions and potential failure to meet the commander’s objectives and/or desired end state. (AFI 10-701)

friendly activity. A function, mission, action, or collection of actions conducted by friendly forces as part of an operation that an operations security officer conceptually groups in order to conduct analysis and apply the operations security process. (JFSC DOPC)

impact. Cost in time, resources, personnel or interference with other operations associated with implementing each possible operations security countermeasure versus the potential harmful effects on mission accomplishment resulting from an adversary’s exploitation of a particular vulnerability. (NTRP 1-02)

indicator. Data derived from friendly detectable actions and open-source information that an adversary can interpret and piece together to reach conclusions or estimates of friendly intentions, capabilities, or activities. (JP 3-13.3)

information environment. The aggregate of individuals, organizations, and systems that collect, process, disseminate, or act on information. (JP 3-13)

information-related capability. A tool, technique, or activity employed within a dimension of the information environment that can be used to create effects and operationally desirable conditions. (JP 3-13)

information superiority. The operational advantage derived from the ability to collect, process, and disseminate an uninterrupted flow of information while exploiting or denying an adversary's ability to do the same. (JP 3-13)

information warfare. The integrated employment of Navy's information-based capabilities (communications, networks, intelligence, oceanography, meteorology, cryptology, electronic warfare, cyberspace operations, and space) to degrade, deny, deceive, or destroy an enemy's information environment or to enhance the effectiveness of friendly operations. (NTRP 1-02)

military deception. Actions executed to deliberately mislead adversary military, paramilitary, or violent extremist organization decision makers, thereby causing the adversary to take specific actions (or inactions) that will contribute to the accomplishment of the friendly mission. (JP 3-13.4)

observable. Activities apparent to observers and/or collectors that might be analyzed and used by the decision maker. The combination of an indicator and an opposing force conduit or open-source reporting. (AFI 10-701)

open-source research. Monitoring publically available information to identify potential disclosures of critical information and indicators. Open-source research does not produce intelligence. (SECNAV 3070.2A)

operational aspects. An operational feature, detail, or conclusion that can be derived by adversary collection and analysis of friendly activities. The more operational aspects revealed by observable friendly activities, the greater the value to the adversary as an indicator. Operational aspects used are presence, capability, strength, intent, readiness, location, timing, and method. (JFSC DOPC)

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 3-0)

operations security. A capability that identifies and controls critical information, indicators of friendly force actions attendant to military operations, and incorporates countermeasures to reduce the risk of an adversary exploiting vulnerabilities. Also called OPSEC. (JP 3-13.3)

operations security assessment. An evaluative process to determine the likelihood that critical information can be protected from the adversary's intelligence. (JP 3-13.3)

operations security countermeasure. Methods and means to gain and maintain essential secrecy about critical information. (JP 3-13.3)

OPSEC countermeasure. Planned offensive action taken to affect collection, analysis, delivery, or interpretation of information that impacts content and flow of critical information and indicators. (SECNAV 3070.2A)

OPSEC measure. Planned action to conceal or protect critical information and indicators from disclosure, observation, or detection and protect them from collection; generally defensive in nature. (SECNAV 3070.2A)

perspective. How a friendly activity is analyzed relative to the potential for the adversary to derive aspects of friendly operations that might prove useful to the decision maker. The three analytical perspectives are isolation, sequence, and context. (JFSC DOPC)

physical indicator. Unique properties that can be collected or analyzed using the human senses (including sensors that replicate the human eye). Collection normally involves line of sight. (JFSC DOPC)

publicly available information. Information that has been published or broadcast for public consumption, is available on request to the public, is accessible on-line or otherwise to the public, is available to the public by subscription or purchase, could be seen or heard by a casual observer, is made available at a meeting open to the public, or is obtained by visiting a place or attending an event that is open to the public. (DODD 3115.18)

repackaging. An operations security technique used to make one profile resemble another existing or new profile by addition or subtraction of visible signatures or changes in the normal sequence of activities. Repackaging can be used to conceal or to generate exploitable contrasts. (JFSC DOPC)

risk. A measure of the potential degree to which protected information is subject to loss through adversary exploitation. (DODM 5205.02)

risk assessment. A process of evaluating the risks to information based on susceptibility to intelligence collection and the anticipated severity of loss. (DODM 5205.02)

risk management. The process of identifying, assessing, and controlling risks by making decisions that balance risk costs with mission benefits. Costs may be measured in financial cost, loss of assets, loss of information, or loss of reputation. (DODM 5205.02)

technical indicator. Unique electromagnetic, infrared, thermal, or other emanations not readily discernable by human senses. Adversary attribution of a technical signature to a friendly activity or capability normally involves association. (JFSC DOPC)

threat analysis. A process that examines an adversary's technical and operational capabilities, motivation, and intentions, designed to detect and exploit vulnerabilities. (DODM 5205.02)

vulnerability. A condition in which friendly actions provide operations security indicators that may be obtained and accurately evaluated by an adversary in time to provide a basis for effective adversary decision making. (JP 3-13.3)

vulnerability analysis. A process that examines a friendly operation or activity from the point of view of an adversary, seeking ways in which the adversary might determine critical information in time to disrupt or defeat the operation or activity. (DODM 5205.02)

INTENTIONALLY BLANK

LIST OF ACRONYMS AND ABBREVIATIONS

AFI	Air Force instruction
AO	area of operations
AOR	area of responsibility
BLUF	bottom line up front
CAT	close access team
CCDR	combatant commander
CI	counterintelligence
CII	critical information and indicators
CIIL	critical information and indicator list
CIL	critical information list
CMD	command
CO	commanding officer
COA	course of action
COMSEC	communications security
COMUSFLTFORCOMINST	Commander, United States Fleet Forces Command instruction
CONOPS	Concept of operations
CPI	critical program information
CSG	carrier strike group
CTF	commander, task force
CUI	controlled unclassified information
DCO	defensive cyberspace operations
DD	Department of Defense form
DFARS	Defense Federal Acquisition Regulation Supplement
DIA	Defense Intelligence Agency
DISO	deception in support of operations security
DOD	Department of Defense
DODD	Department of Defense directive
DODI	Department of Defense instruction
DODM	Department of Defense manual
DON	Department of the Navy
DOPC	Defense Operations Security Planners Course
EA	electronic attack
EMCON	emission control
EPRM	Enterprise Protection Risk Management
EW	electromagnetic warfare
EXORD	execute order
FA	friendly activity
FAR	Federal Acquisition Regulation
FBI	Federal Bureau of Investigation

FOIA	Freedom of Information Act
FSO	facility security officer
GEOINT	geospatial intelligence
H	high
HQ	headquarters
HUMINT	human intelligence
IA	information assurance
IE	information environment
IO	information operations
IRC	information-related capability
ISIC	immediate superior in command
ISRT	intelligence, surveillance, reconnaissance, and targeting
IW	information warfare
IWC	information warfare commander
JCMA	joint communications security monitoring activity
JFSC	Joint Forces Staff College
JP	joint publication
L	low
M	medium
MASINT	measurement and signature intelligence
MH	medium high
MILDEC	military deception
ML	medium low
MOE	measure of effectiveness
MOP	measure of performance
N2	intelligence
N39	Navy staff information operations
NA	not applicable
NCIS	Naval Criminal Investigative Service
NIWTG	Navy Information Warfare Training Group
NOST	Naval Operations Security Support Team
NPP	Navy planning process
NRT	Navy red team
NSA	National Security Agency
NSDD	national security decision directive
NTISSD	National Telecommunication and Information Security System directive
NTRP	Navy tactical reference publication
NTTP	Navy tactics, techniques, and procedures
NVA	North Vietnamese Army
NWL	Navy Warfare Library
NWP	Navy warfare publication
OCO	offensive cyberspace operations

OE	operational environment
OFRP	optimized fleet response plan
OLW	operational level of warfare
OPLAN	operation plan
OPNAVINST	Chief of Naval Operations instruction
OPORD	operation order
OPSEC	operations security
OSINT	open-source intelligence
OSR	open-source research
OWG	operations security working group
PA	public affairs
PAI	publicly available information
PBED	plan, brief, execute, debrief
PCMS	passive countermeasures system
PII	personally identifiable information
POA&M	plan of action and milestones
PWS	performance work statement
RF	radio frequency
RFI	request for information
SAPCE	signatures, associations, profiles, contrasts, and exposure
SECNAVINST	Secretary of the Navy instruction
SF	standard form
SIGCON	signature control
SIGINT	signals intelligence
SIPRNET	SECRET Internet Protocol Router Network
SME	subject matter expert
SOP	standard operating procedure
SRRB	service requirements review board
STO	special technical operations
TA	threat assessment
TTP	tactics, techniques, and procedures
U.S.	United States
U.S.C.	United States Code
WWII	World War II

INTENTIONALLY BLANK

LIST OF EFFECTIVE PAGES

Effective Pages	Page Numbers
DEC 2022	1 thru 10
DEC 2022	1-1, 1-2
DEC 2022	2-1 thru 2-6
DEC 2022	3-1 thru 3-6
DEC 2022	4-1 thru 4-8
DEC 2022	5-1 thru 5-6
DEC 2022	6-1 thru 6-12
DEC 2022	A-1 thru A-4
DEC 2022	B-1 thru B-4
DEC 2022	C-1, C-2
DEC 2022	D-1 thru D-16
DEC 2022	E-1 thru E-4
DEC 2022	F-1, F-2
DEC 2022	G-1 thru G-8
DEC 2022	H-1 thru H-8
DEC 2022	Reference-1, Reference-2
DEC 2022	Glossary-1 thru Glossary-4
DEC 2022	LOAA-1 thru LOAA-4
DEC 2022	LEP-1, LEP-2

INTENTIONALLY BLANK

NTTP 3-13.3
DEC 2022