Joint Publication 3-13.3

Operations Security

04 January 2012

PREFACE

1. Scope

This publication provides joint doctrine for planning, executing, and assessing operations security in joint operations.

2. Purpose

This publication has been prepared under the direction of the Chairman of the Joint Chiefs of Staff. It sets forth joint doctrine to govern the activities and performance of the Armed Forces of the United States in operations and provides the doctrinal basis for interagency coordination and for US military involvement in multinational operations. It provides military guidance for the exercise of authority by combatant commanders and other joint force commanders (JFCs) and prescribes joint doctrine for operations and training. It also provides military guidance for use by the Armed Forces in preparing their appropriate plans. It is not the intent of this publication to restrict the authority of the JFC from organizing the force and executing the mission in a manner the JFC deems most appropriate to ensure unity of effort in the accomplishment of the overall objective.

3. Application

a. Joint doctrine established in this publication applies to the combatant commands, subunified commands, joint task forces, subordinate components of these commands, and the Services.

b. The guidance in this publication is authoritative; as such, this doctrine will be followed except when, in the judgment of the commander, exceptional circumstances dictate otherwise. If conflicts arise between the contents of this publication and the contents of Service publications, this publication will take precedence unless the Chairman of the Joint Chiefs of Staff, normally in coordination with the other members of the Joint Chiefs of Staff, has provided more current and specific guidance. Commanders of forces operating as part of

a multinational (alliance or coalition) military command should follow multinational doctrine and procedures ratified by the United States. For doctrine and procedures not ratified by the United States, commanders should evaluate and follow the multinational command's doctrine and procedures, where applicable and consistent with US law, regulations, and doctrine.

For the Chairman of the Joint Chiefs of Staff:

WILLIAM E. GORTNEY
VADM, USN
Director, Joint Staff

SUMMARY OF CHANGES
REVISION OF JOINT PUBLICATION 3-13.3
DATED 29 JUNE 2006

- **Restructures document format, removing key sections from appendixes and placing them within appropriate chapters.**

- **Adds figure providing examples of critical information during threat analysis in the operations security (OPSEC) process.**

- **Increases the components of OPSEC risk assessment to three by adding a second step in which the commander and staff estimate the impact on operations associated with implementing each possible OPSEC countermeasure.**

- **Adds section on joint and interagency planning during OPSEC planning.**

- **Adds a section on intergovernmental and nongovernmental organization considerations during OPSEC planning.**

- **Redefines the terminology for OPSEC assessments: Changes the OPSEC command assessment to an OPSEC assessment and OPSEC formal assessment to an OPSEC survey.**

- **States the requirement for an OPSEC assessment to be conducted annually, while an OPSEC survey will be conducted every three years.**

- **Adds additional OPSEC countermeasures: physical attack and electronic warfare as an operational and logistic measure, awareness of OPSEC vulnerabilities presented by online social networking, and shredding of documents as administrative measures.**

- **Adds a new appendix, "Sample Operations Plan."**

- **Updates references and acronyms.**

TABLE OF CONTENTS

PAGE

EXECUTIVE SUMMARY vii

CHAPTER I
GENERAL

- Policy I-1
- Operational Context I-1
- Purpose of Operations Security I-2
- Operations Security and Intelligence I-2
- Characteristics of Operations Security I-3
- Operations Security and Information Operations I-4
- Operations Security Responsibilities I-4

CHAPTER II
THE OPERATIONS SECURITY PROCESS

- General II-1
- Identify Critical Information II-1
- Threat Analysis II-2
- Vulnerability Analysis II-4
- Risk Assessment II-5
- Apply Operations Security Countermeasures II-6

CHAPTER III
OPERATIONS SECURITY PLANNING

- General III-1
- Operations Security Factors III-1
- Operations Security Indicators III-3
- Operations Security Countermeasures III-6
- Planning Coordination III-9
- Joint and Interagency Planning III-10
- Multinational Planning III-10
- Intergovernmental and Nongovernmental Organization Considerations III-11

CHAPTER IV
OPERATIONS SECURITY ASSESSMENTS

- Assessments and Surveys IV-1
- Assessment Planning IV-4
- Assessment Execution IV-6
- Analysis and Reporting IV-8

APPENDIX

A	Operations Security Indicators	A-1
B	Functional Outlines and Profiles	B-1
C	Sample Operations Security Plan	C-1
D	References	D-1
E	Administrative Instructions	E-1

GLOSSARY

Part I	Abbreviations and Acronyms	GL-1
Part II	Terms and Definitions	GL-3

FIGURE

II-1	The Operations Security Process	II-2
II-2	Examples of Critical Information	II-3
IV-1	Assessment–Survey Comparison	IV-3

EXECUTIVE SUMMARY
COMMANDER'S OVERVIEW

- **Provides a General Overview of Operations Security**
- **Describes the Operations Security Process**
- **Explains Operations Security Planning**
- **Discusses Operations Security Assessments, Surveys, and Reporting**

Operations Security

Operational Context

Joint forces often display personnel, organizations, assets, and actions to public view and to a variety of adversary intelligence collection activities, including sensors and systems. Joint forces can be under observation at their peacetime bases and locations, in training or exercises, while moving, or when deployed to the field conducting actual operations. In addition, the adversary could compile and correlate enough information to facilitate predicting and countering US operations.

Purpose of Operations Security (OPSEC)

The purpose of operations security (OPSEC) is to **reduce the vulnerability** of US and multinational forces from successful adversary exploitation of critical information. OPSEC applies to all activities that prepare, sustain, or employ forces. The **OPSEC process is a systematic method used to** identify, control, and protect critical information and subsequently analyze friendly actions associated with military operations.

OPSEC and Intelligence

Tailored to the OPSEC process, joint intelligence preparation of the operational environment is a useful methodology for intelligence professionals to support the OPSEC planner. The intelligence professional will perform mission analysis on friendly operations. This provides great insight into potential areas where the adversary could collect information and the identity of essential elements of friendly information (EEFIs). Identification of EEFIs will assist the OPSEC planner in ensuring all OPSEC-related critical unclassified information is included in the critical information list.

Characteristics of OPSEC

OPSEC's most important characteristic is that **it is a process. It is an analytical process that can be applied to any operation or activity** for the purpose of denying critical information to an adversary. Unlike security programs that seek to protect classified information and controlled unclassified information, OPSEC is concerned with **identifying, controlling,** and **protecting unclassified information** that is associated with specific military operations and activities.

OPSEC and Information Operations

OPSEC as a capability of information operations (IO) denies the adversary the information needed to correctly assess friendly capabilities and intentions. It is also a tool, hampering the adversary's use of its own information systems and processes and providing the necessary support to all friendly IO capabilities.

OPSEC Responsibilities

The **Chairman of the Joint Chiefs of Staff (CJCS)** advises the Secretary of Defense concerning OPSEC support to the combatant commands. The CJCS provides procedures for OPSEC planning in the Joint Operation Planning and Execution System and ensures that appropriate OPSEC countermeasures are implemented during CJCS operations and exercises.

Service Chiefs provide Service OPSEC policy, doctrine, and planning procedures consistent with joint OPSEC policy, doctrine, and guidance. They provide OPSEC-related training to all Service members and designate an OPSEC program manager in the Service headquarters.

Combatant commanders (CCDRs) provide OPSEC guidance for all operations, exercises, and other joint activities of the command. CCDRs conduct OPSEC planning in accordance with applicable policy and plan for and execute OPSEC countermeasures in support of assigned missions.

The **OPSEC program manager's** primary function is to advise the Service Chief or CCDR as applicable on OPSEC matters. Program managers coordinate the development of the OPSEC-related portions of operation plans and operation orders and develop and maintain the organization's OPSEC program, to include writing the organization's policy and guidance documents.

The Operations Security Process

OPSEC Process

Use of the process ensures that the resulting OPSEC countermeasures address all significant aspects of the particular situation and are balanced against operational requirements. **The OPSEC process consists of five distinct actions:** identification of critical information, analysis of threats, analysis of vulnerabilities, assessment of risk, and application of appropriate OPSEC countermeasures.

Identify Critical Information

The **identification of critical information is a key part of the OPSEC process because it focuses the remainder of the OPSEC process on protecting vital information** rather than attempting to protect all unclassified information. Critical information answers key questions likely to be asked by adversaries about specific friendly intentions, capabilities, and activities necessary for adversaries to plan and act effectively against friendly mission accomplishment.

Threat Analysis

Threat analysis involves the research and analysis of **intelligence, counterintelligence,** and **open-source information** to identify the likely adversaries to the planned operation.

Vulnerability Analysis

The purpose of this vulnerability analysis is to **identify an operation's or activity's vulnerabilities.** A vulnerability exists when the adversary is capable of collecting critical information, correctly analyzing it, and then taking timely action.

Risk Assessment

This action has three components. First, planners **analyze the vulnerabilities** identified in the previous action **and identify possible OPSEC countermeasures** for each vulnerability. Second, the commander and staff **estimate the impact on operations** such as cost in time, resources, personnel, or interference with other operations associated with implementing each possible OPSEC countermeasure versus the potential harmful effects on mission accomplishment resulting from an adversary's exploitation of a particular vulnerability. Third, the commander and staff **select specific OPSEC countermeasures for execution** based upon a risk assessment done by the commander and staff.

Apply OPSEC Countermeasures

The command implements the OPSEC countermeasures selected in the risk assessment process or, in the case of planned future operations and activities, includes the measures in specific operations plans. The adversary's reaction is monitored to determine the countermeasures' effectiveness and to provide feedback.

Operations Security Planning

Effective OPSEC

In order to prevent adversaries (or potential adversaries) from gaining critical information concerning friendly operations, joint forces must plan and execute OPSEC. To be effective, OPSEC must be considered as early as possible during mission planning and appropriately revised to keep pace with any changes in current operations and adversarial threats.

OPSEC Factors

Some of the factors that must be considered when conducting OPSEC planning:

- OPSEC planning guidance should be provided as part of the commander's planning guidance.
- OPSEC is an operations function, not a security function.
- OPSEC should be integrated into the IO cell.
- OPSEC planning should focus on identifying and protecting critical information.

OPSEC Indicators

OPSEC indicators are friendly detectable actions and open-source information that can be interpreted or pieced together by an adversary to derive critical information. These indicators must be continuously analyzed and considered during planning.

OPSEC Countermeasures

Development of specific OPSEC countermeasures is as varied as the specific vulnerabilities they are designed to offset. These include operational and logistic measures, technical measures, administrative measures, and operations and military deception.

Planning Coordination

Joint force commanders normally establish a joint planning group (JPG). Early and continuous exchange of information and close coordination of planning activities between the JPG and the OPSEC representative are essential to successfully integrating OPSEC into planning and execution. OPSEC planning is always done in

conjunction with joint operation planning and is a part of the overall IO planning effort.

Joint and Interagency Planning

The current operational environment may require coordination of OPSEC efforts with other government departments and agencies, such as the Central Intelligence Agency, Department of Homeland Security, Department of Energy, or Federal Bureau of Investigation.

Multinational Planning

US military operations often are conducted with the armed forces of other nations in pursuit of common objectives. OPSEC countermeasures that apply to joint operations are also appropriate for multinational situations.

Intergovernmental and Nongovernmental Organization Considerations

Intergovernmental organizations (IGOs) and nongovernmental organizations (NGOs) are prominent participants in the current operating environment, particularly in foreign humanitarian assistance, peace, and stability operations. **Military planners must consider and assess potential OPSEC vulnerabilities and threats whenever IGOs and NGOs are present in the operational area.** Joint force representatives in the civil-military operations center or joint civil-military operations task force must be vigilant in protecting critical information when coordinating with various IGOs and NGOs.

Operations Security Assessments

Assessments and Surveys

OPSEC assessments are conducted annually to evaluate an operation, activity, exercise, or support function to determine the likelihood that critical information can be protected from the adversary's intelligence collection systems. An OPSEC assessment is normally run by the OPSEC program manager and performed by the unit's OPSEC working group. The scope of an OPSEC assessment is usually limited to events and/or activities within that organization.

A survey usually requires a team of external subject matter experts from multiple disciplines to simulate adversary intelligence processes. An OPSEC survey should focus on the organization's ability to adequately protect critical information from adversary intelligence exploitation during planning, preparation, execution, and post-execution phases of any operation or program. A survey is required every three years.

Assessment Planning

The required lead time to prepare for an assessment depends on the nature and complexity of the operation and activities assessed (combat operations, peacetime operational activity, or other type of operation). Allot sufficient time in the planning phase for a thorough review of pertinent documentation, for formal and informal coordination and discussions, and for careful preparation of a functional outline.

Assessment Execution

Data collection begins in the planning phase with a review of associated documentation. During the assessment phase, interviews with personnel directly involved in the operation, together with observations and document collection, are the primary means of data collection.

Analysis and Reporting

During analysis and reporting, the OPSEC team correlates the data acquired by individual members with information from any empirical studies conducted in conjunction with the assessment. The report of the OPSEC assessment is addressed to the commander of the assessed operation or activity. The report should provide a discussion of identified critical information, indicators, adversaries and their intelligence capabilities, OPSEC vulnerabilities, risk analysis, and recommended OPSEC countermeasures to eliminate or reduce the vulnerabilities.

CONCLUSION

This publication provides joint doctrine for planning, executing, and assessing OPSEC in joint operations.

CHAPTER I
GENERAL

"If I am able to determine the enemy's dispositions while at the same time I conceal my own, then I can concentrate and he must divide."

Sun Tzu, The *Art of War*, 400–320 BC

1. Policy

Policy for joint operations security (OPSEC) is established by the Chairman of the Joint Chiefs of Staff Instruction (CJCSI) 3213.01C, *Joint Operations Security*.

2. Operational Context

a. Joint forces often display personnel, organizations, assets, and actions to public view and to a variety of adversary intelligence collection activities, including sensors and systems. Joint forces can be under observation at their peacetime bases and locations, in training or exercises, while moving, or when deployed to the field conducting actual operations. Frequently, when a force performs a particular activity or operation a number of times, it establishes a pattern of behavior. Within this pattern, certain unique, particular, or special types of information might be associated with an activity or operation. Even though this information may be unclassified, it can expose significant US military operations to observation and/or interdiction. In addition, the adversary could compile and correlate enough information to facilitate predicting and countering US operations.

b. An **indicator** is data derived from friendly detectable actions and open-source information that adversaries can interpret and piece together to reach conclusions or estimates of critical or classified information concerning friendly intentions, capabilities, or activities. Selected indicators can be developed into an analytical **model** or profile of how a force prepares and how it operates. An **indication** is an observed specific occurrence or instance of an indicator.

c. Adversary intelligence personnel continuously analyze and interpret collected information to validate and/or refine the model. As adversary analysts apply more information to the analytical model, the likelihood increases that the analytical model will replicate the observed force. Thus, current and future capabilities and courses of action (COA) can be revealed and compromised. **Critical information** consists of specific facts about friendly intentions, capabilities, and activities needed by adversaries to plan and act effectively against friendly mission accomplishment. Critical information could be, and usually is, unclassified.

d. Commanders cannot limit their protection efforts to a particular operational area or threat. With continuing rapid advancement and global use of communications systems and informational technology, easily obtainable technical collection tools, and the growing use of the Internet and various social and mass media outlets, the ability to collect critical

information virtually from anywhere in the world and threaten US military operations continues to expand. To prevent or reduce successful adversary collection and exploitation of US critical information, the commander should formulate a prudent, practical, timely, and effective OPSEC program. Additionally, the commander's OPSEC program should be dynamic and continuously updated to enable application of the OPSEC process to mitigate unacceptable risks in a changing operational environment.

e. OPSEC considerations must also be observed while working in the interagency environment.

3. Purpose of Operations Security

a. The purpose of OPSEC is to **reduce the vulnerability** of US and multinational forces from successful adversary exploitation of critical information. OPSEC applies to all activities that prepare, sustain, or employ forces.

b. The **OPSEC process is a systematic method used to** identify, control, and protect critical information and subsequently analyze friendly actions associated with military operations and other activities to:

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

(2) Determine what specific indications could be collected, analyzed, and interpreted to derive critical information in time to be useful to adversaries.

(3) Select countermeasures that eliminate or reduce vulnerability or indicators to observation and exploitation.

(4) Avoid patterns of behavior, whenever feasible, and thus preclude the possibility of adversary intelligence constructing an accurate model.

(5) Prevent the display or collection of critical information, especially during preparation for and execution of actual operations.

(6) Avoid drastic changes as OPSEC countermeasures are implemented. Changes in procedures alone will indicate to the adversary that there is an operation or exercise starting.

4. Operations Security and Intelligence

a. Intelligence plays a key role in the OPSEC process. Joint intelligence preparation of the operational environment (JIPOE) is the analytical process used by joint intelligence organizations to produce intelligence assessments, estimates, and other intelligence products in support of the joint force commander's (JFC's) decision-making process. Tailored to the OPSEC process, JIPOE is a useful methodology for intelligence professionals to support the OPSEC planner.

b. The first step of JIPOE is to define the operational environment—operational areas and areas of interest. In the case of OPSEC and protecting critical unclassified information, the operational environment can be considerably larger where an adversary intelligence organization can collect on friendly activities. Also during this step, the intelligence professional will perform mission analysis on friendly operations. This provides great insight into potential areas where the adversary could collect information as well as the identification of essential elements of friendly information (EEFIs). Identification of EEFIs will assist the OPSEC planner in ensuring all OPSEC-related critical unclassified information is included in the critical information list (CIL).

c. The second step of the JIPOE process is to describe the impact of the operational environment on adversary, friendly, and neutral military capabilities and broad COAs. From an OPSEC perspective, this could entail the expected physical, cognitive, and informational impact from the friendly mission. If a unit's deployment had not been previously announced, and then is, what impact does that have? Is it the same to say that a unit is deploying in the second half of the year or on October the 12th at noon from the local airport? What friendly actions can be taken to minimize the impact of releasing that type of information? What information needs to be protected?

d. The third step of JIPOE involves evaluating the adversary. For OPSEC purposes, what capabilities does the adversary have to collect on friendly operations? Does it have a robust open-source, human intelligence (HUMINT) or signals intelligence (SIGINT) capability? What are its tactics, techniques, and procedures? What are its critical capabilities and vulnerabilities? Intelligence support to OPSEC personnel will often compile the adversary's capabilities into a threat brief to present to OPSEC planners.

e. The fourth and final step of the JIPOE process is to determine the adversary's COAs. The purpose of step four is to identify the COA the adversary is most likely to adopt and the COA that would be most dangerous to the friendly force or to mission accomplishment. In terms of OPSEC, this amounts to where the adversary will most likely deploy its resources to collect information on the friendly force.

For additional information on JIPOE, see Joint Publication (JP) 2-01.3, Joint Intelligence Preparation of the Operational Environment.

5. Characteristics of Operations Security

a. OPSEC's most important characteristic is that **it is a process.** OPSEC is not a collection of specific rules and instructions. **It is an analytical process that can be applied to any operation or activity** for the purpose of denying critical information to an adversary.

b. Unlike security programs that seek to protect classified information and controlled unclassified information (CUI), OPSEC is concerned with **identifying, controlling,** and **protecting unclassified information** that is associated with specific military operations and activities. While some of the critical information in an OPSEC program may be CUI, most of the critical information is situation dependent. **OPSEC and security programs must be closely coordinated** to ensure appropriate aspects of military operations are protected.

OPSEC and other security programs (i.e., information security, physical security, personnel security, industrial security, acquisition security, emissions security, information assurance (IA), communications security [COMSEC], etc.) are complementary and should not be confused as being the same.

c. Some level of risk must be assumed when choosing whether to execute OPSEC countermeasures. OPSEC countermeasures, in most cases, involve the expenditure of resources. In choosing to execute particular OPSEC countermeasures, commanders determine if the estimated **gain in security outweighs the costs in resources.** If commanders decide not to execute certain measures because the costs outweigh the gain, then they are assuming risk. The OPSEC process demands that decision makers directly address what is acceptable risk and how much risk the decision makers are willing to assume.

6. Operations Security and Information Operations

OPSEC as a capability of information operations (IO) denies the adversary the information needed to correctly assess friendly capabilities and intentions. It is also a tool, hampering the adversary's use of its own information systems and processes and providing the necessary support to all friendly IO capabilities. In particular, OPSEC complements military deception (MILDEC) by denying an adversary information required to both assess a real plan and to disprove a deception plan. OPSEC and MILDEC have the same ultimate goal—affecting the adversary's decision-making process and leading it to an erroneous decision. OPSEC does it by concealing important information, and MILDEC does it by putting misleading information into the environment. These are two related processes. For IO capabilities that exploit new opportunities and vulnerabilities, such as electronic warfare and computer network attack, OPSEC is essential to ensure friendly capabilities that might be easily countered are not compromised. The process of identifying critical information and applying measures to mask them from disclosure to adversaries is only one part of a defense-in-depth approach to securing friendly information. To be effective, other types of security must complement OPSEC. Examples of other types of security include physical security, programs in IA, computer network defense, and personnel programs that screen personnel and limit authorized access. In particular, COMSEC plays a vital role in OPSEC. While COMSEC's primary purpose is to protect classified materials, it can assist with identifying vulnerabilities to loss of critical information through monitoring communications within legal constraints.

For further information on IO, refer to JP 3-13, Information Operations.

7. Operations Security Responsibilities

a. **Chairman of the Joint Chiefs of Staff (CJCS).** The CJCS advises the Secretary of Defense concerning OPSEC support to the combatant commands. The CJCS is responsible for providing joint OPSEC policy and doctrine. The CJCS also provides guidance to the combatant commanders (CCDRs) for the annual review and evaluation of their OPSEC programs. The CJCS provides procedures for OPSEC planning in the Adaptive Planning and

Execution (APEX) system and ensures that appropriate OPSEC countermeasures are implemented during CJCS operations and exercises.

b. **Director for Operations (J-3), Joint Staff**

(1) The J-3 executes primary Joint Staff responsibility for OPSEC and designates OPSEC staff positions for the Joint Staff. The J-3 provides guidance for input of OPSEC lessons learned into the Joint Lessons Learned Information System database. The J-3 supports OPSEC planning and training by the Joint Staff, Services, combatant commands, and Department of Defense (DOD) agencies. The J-3 also assists commands and joint agencies in arranging and scheduling Interagency Operations Security Support Staff (IOSS) or joint information operations warfare center/joint OPSEC support element (JIOWC/JOSE) participation in OPSEC assessments and surveys.

(2) The J-3 coordinates with the Joint Staff, Director for Strategic Plans and Policy (J-5), to ensure that OPSEC is adequately addressed and evaluated in operation plans (OPLANs) and operation plans in concept format. The J-3 coordinates with the Joint Staff, Director for Joint Force Development (J-7), to ensure that OPSEC is adequately addressed and evaluated in training and exercises. The J-3 assigns an OPSEC liaison officer (LNO) during periods of crisis and during CJCS exercises to assist all Joint Staff elements in integrating OPSEC into crisis management planning efforts. The OPSEC LNO will also serve as a point of contact to coordinate OPSEC issues with the combatant commands, DOD agencies, and Services. The J-3 establishes the operations security executive groups (OEGs) as necessary, composed of members of the Joint Staff, Services, and appropriate agencies, to address specific OPSEC issues, such as problems relating to OPSEC programs that involve multiple commands or agencies. The J-3 also coordinates with the National Security Agency (NSA), IOSS, the Defense Threat Reduction Agency, and JIOWC/JOSE for OPSEC support.

(3) The J-3 maintains a Joint OPSEC Support Element to provide OPSEC training, program review, surveys, and plans and exercise support to the CCDRs. The J-3 provides OPSEC advocacy for the CCDRs.

c. **Service Chiefs**

(1) Service Chiefs provide Service OPSEC policy, doctrine, and planning procedures consistent with joint OPSEC policy, doctrine, and guidance. They provide OPSEC-related training to all Service members and designate an OPSEC program manager in the Service headquarters. The Service Chiefs designate representatives to Joint Staff OEGs, when required.

(2) The Service Chiefs provide OPSEC lessons learned to the Joint Staff J-3 for inclusion in the OPSEC lessons learned database and provide Joint Staff J-3 copies of all current Service OPSEC program directives and/or policy implementation documents.

d. **Combatant Commanders**

(1) CCDRs provide OPSEC guidance for all operations, exercises, and other joint activities of the command. CCDRs conduct OPSEC planning in accordance with applicable policy and plan for and execute OPSEC countermeasures in support of assigned missions.

They coordinate OPSEC countermeasures and their execution with JIOWC/JOSE or combatant commands and other commands and agencies of those activities that cross command boundaries and report any unresolved issues to the Joint Staff J-3 for assistance. CCDRs conduct OPSEC assessments and surveys in support of command operations, conduct annual OPSEC reviews, and identify areas requiring additional CJCS guidance, assistance, or clarification to the Joint Staff J-3. CCDRs also designate an OPSEC program manager in the command headquarters.

(2) CCDRS provide OPSEC lessons learned to the Joint Staff J-3 for inclusion in the joint OPSEC lessons learned database via the Joint Lessons Learned Information System, and provide Joint Staff J-3 copies of all current command OPSEC program directives and/or policy implementation documents.

e. **OPSEC Program Manager**

(1) The OPSEC program manager's primary function is to advise the Service Chief or CCDR as applicable on OPSEC matters. The OPSEC program managers coordinate the development of the OPSEC-related portions of OPLANs and operation orders (OPORDs) and develop and maintain the organization's OPSEC program, to include writing the organization's policy and guidance documents. The OPSEC program managers manage organizational OPSEC education and awareness training for all assigned personnel, coordinate the conduct of OPSEC assessments and surveys, and conduct the organization's annual OPSEC review.

(2) The OPSEC program manager coordinates with appropriate intelligence, counterintelligence (CI) support, counterespionage, force protection, antiterrorism, security, and public affairs (PA). They also coordinate with security program managers and coordinate the development and integration of OPSEC into IO supporting and related capabilities.

(3) The OPSEC program manager manages the OPSEC working group to address specific OPSEC issues and monitor/promote OPSEC awareness and ensures procedures are in place to control critical information and indicators.

f. **Director, Defense Intelligence Agency (DIA).** The Director, DIA, establishes and maintains an OPSEC training program for DIA personnel (civilian, military, and contractor) and attendees at the National Defense Intelligence College, designates an agency OPSEC program manager, and designates representatives to Joint Staff OEGs, as required. The Director, DIA, also identifies, reviews, and validates DIA and other DOD threat assessment documents for Joint Staff use. The Director, DIA, conducts analysis of the foreign intelligence collection threat for required nations and organizations for use in OPSEC planning and for monitoring the effectiveness of implemented OPSEC countermeasures and provide results to the CJCS, CCDRs, Service Chiefs, and heads of the DOD agencies.

g. **Director, National Security Agency**

(1) The Director, National Security Agency (DIRNSA), assists DOD and others with a national security mission in establishing OPSEC programs, usually through the joint

or Service OPSEC support element, as requested. DIRNSA provides interagency OPSEC training courses and designates representative to Joint Staff OEGs, as required.

(2) DIRNSA collaborates with the heads of the DOD components by providing:

(a) Technical OPSEC survey support to DOD components to assist them in identifying their OPSEC vulnerabilities.

(b) Recommendations relating to doctrine, methods, and procedures to minimize those vulnerabilities, when requested.

(c) Communications and computer security support for OPSEC surveys.

(d) SIGINT support for OPSEC threat development.

(e) COMSEC monitoring services to DOD elements through the joint COMSEC monitoring activity.

h. **Heads of Other DOD Agencies and Joint Activities.** The heads of other DOD agencies and joint activities designate an agency OPSEC program manager. They coordinate OPSEC programs and activities with commands and other agencies, as required, and provide representatives to Joint Staff OEGs, as required.

Intentionally Blank

CHAPTER II

"Little minds try to defend everything at once, but sensible people look at the main point only; they parry the worst blows and stand a little hurt if thereby they avoid a greater one. If you try to hold everything, you hold nothing."

Frederick the Great
Instructions for His Generals, 1747

THE OPERATIONS SECURITY PROCESS

1. General

a. **OPSEC planning is based upon the OPSEC process.** This process, when used in conjunction with the joint planning process, provides the information required to write the OPSEC section of any plan or order. OPSEC planning is done in close coordination with the overall IO planning effort.

b. The OPSEC process is applicable across the range of military operations. Use of the process ensures that the resulting OPSEC countermeasures address all significant aspects of the particular situation and are balanced against operational requirements. OPSEC is a continuous process. **The OPSEC process (Figure II-1) consists of five distinct actions:** identification of critical information, analysis of threats, analysis of vulnerabilities, assessment of risk, and application of appropriate OPSEC countermeasures. These OPSEC actions are applied continuously during OPSEC planning. In dynamic situations, however, individual actions may be reevaluated at any time. New information about the adversary's intelligence collection capabilities, for instance, would require a new analysis of threats.

c. An understanding of the following terms is required before the process can be explained.

(1) **Critical Information.** These are specific facts about friendly intentions, capabilities, and activities needed by adversaries to plan and act effectively against friendly mission accomplishment.

(2) **OPSEC Indicators.** Friendly detectable actions and open-source information that can be interpreted or pieced together by an adversary to derive critical information.

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

2. Identify Critical Information

a. The **identification of critical information is a key part of the OPSEC process because it focuses the remainder of the OPSEC process on protecting vital information**

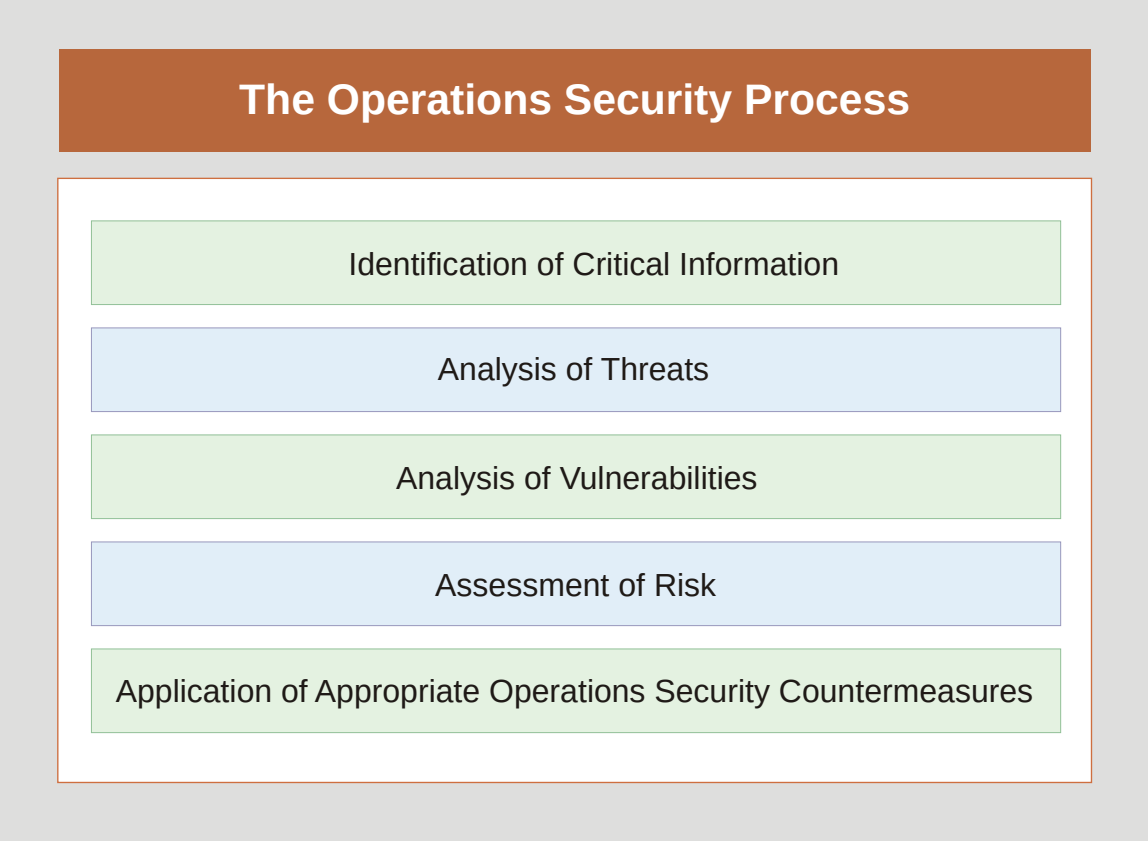


Figure II-1. The Operations Security Process

rather than attempting to protect all unclassified information. Critical information answers key questions likely to be asked by adversaries about specific friendly intentions, capabilities, and activities necessary for adversaries to plan and act effectively against friendly mission accomplishment. There are many areas within an organization where elements of critical information can be obtained. Personnel from outside the organization may also handle portions of its critical information. Therefore it is important to have personnel from each staff section and component involved in the process of identifying critical information. The critical information items should be consolidated into a list known as a CIL.

b. **Critical information is listed in tab C (Operations Security) to appendix 3 (Information Operations) to annex C (Operations) of an OPLAN or OPORD.** Generic CILs (Figure II-2) can be developed beforehand to assist in identifying the specific critical information.

3. Threat Analysis

a. This action involves the research and analysis of **intelligence, CI,** and **open-source information** to identify the likely adversaries to the planned operation.

b. **The operations planners,** working with the intelligence and CI staffs and assisted by the OPSEC program manager, **seek answers to the following threat questions:**

Examples of Critical Information

Model Joint Operation Phases

Shape

- Negotiating positions
- Intelligence verification capabilities
- Forces available
- Targets
- Timing
- Tactics, techniques, and procedures
- Logistic capabilities and constraints
- Critical communication nodes
- Exercise concept plans and operation plans

Deter

- Intentions
- Alert posture
- Military capabilities
- Forces assigned and in reserve
- Target selection
- Tactics, techniques, and procedures
- Logistic capabilities and constraints
- Mobilization
- Purpose, targets and processing of intelligence collection

Seize the Initiative

- Intentions
- Military capability
- Critical communication nodes
- Forces assigned and in reserve
- Target selection
- Tactics, techniques, and procedures
- Logistic capabilities and constraints

Dominate

- Forces assigned and in reserve
- Target selection
- Tactics, techniques, and procedures
- Logistic capabilities and constraints
- Critical communication nodes

Stabilize

- Lines of communications
- Tactics, techniques, and procedures
- Logistic capabilities and constraints
- Critical communication nodes

Enable Civil Authority

- Identity of military forces
- Military support of law enforcement
- Host-nation support
- Capabilities
- Third nation support
- Lines of communications
- Critical communication nodes
- Tactics, techniques, and procedures

Figure II-2. Examples of Critical Information

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

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

(3) What is the adversary's COA for opposing the planned operation? (What actions might the adversary take? Include the most likely COA and COA most dangerous to friendly forces and mission accomplishment.)

(4) What critical information does the adversary already know about the operation? (What information is too late to protect?)

(5) What are the adversary's intelligence collection capabilities?

(6) Who are the affiliates of the adversary, and will they share information?

4. Vulnerability Analysis

a. The purpose of this action is to **identify an operation's or activity's vulnerabilities.** It requires examining each aspect of the planned operation to identify any OPSEC indicators or vulnerabilities that could reveal critical information and then comparing those indicators or vulnerabilities with the adversary's intelligence collection capabilities identified in the previous action. A vulnerability exists when the adversary is capable of collecting critical information, correctly analyzing it, and then taking timely action. The adversary can then exploit that vulnerability to obtain an advantage.

b. Continuing to work with the intelligence personnel, the operations planners seek answers to the following vulnerability questions:

(1) What indicators (friendly actions and open-source information) of critical information not known to the adversary will be created by the friendly activities that will result from the planned operation?

All personnel must understand the adversary's capability to collect information and take operations security countermeasures to deny the use of that capability.

(2) What indicators can the adversary actually collect?

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

(4) Will the application of OPSEC countermeasures introduce more indicators that the adversary will be able to collect?

See Appendix A, "Operations Security Indicators," *for a detailed discussion of OPSEC indicators.*

5. Risk Assessment

a. This action has three components. First, **planners analyze the vulnerabilities** identified in the previous action and **identify possible OPSEC countermeasures** for each vulnerability. Second, the commander and staff estimate the impact to operations such as cost in time, resources, personnel or interference with other operations associated with implementing each possible OPSEC countermeasure versus the potential harmful effects on mission accomplishment resulting from an adversary's exploitation of a particular vulnerability. Third, the commander and staff select **specific OPSEC countermeasures for execution** based upon a risk assessment done by the commander and staff.

b. OPSEC countermeasures reduce the probability of the adversary either observing indicators or exploiting vulnerabilities, being able to correctly analyze the information obtained, and being able to act on this information in a timely manner.

(1) **OPSEC countermeasures can be used** to prevent the adversary from detecting an indicator or exploiting a vulnerability, provide an alternative analysis of a vulnerability or an indicator (prevent the adversary from correctly interpreting the indicator), and/or attack the adversary's collection system.

(2) OPSEC countermeasures include, among other actions, cover, concealment, camouflage, deception, intentional deviations from normal patterns, and direct strikes against the adversary's intelligence system.

(3) **More than one possible measure may be identified for each vulnerability.** Conversely, a single measure may be used for more than one vulnerability. The most desirable OPSEC countermeasures are those that combine the highest possible protection with the least adverse effect on operational effectiveness. Chapter III, "Operations Security Planning," provides a detailed discussion of OPSEC countermeasures.

c. **Risk assessment** requires comparing the estimated cost associated with implementing specific OPSEC countermeasure to the potential harmful effects on mission accomplishment resulting from an adversary's exploitation of a particular vulnerability.

(1) **OPSEC countermeasures may entail some cost** in time, resources, personnel, or interference with normal operations. If the cost to mission effectiveness exceeds the harm that an adversary could inflict, then the application of the measure is inappropriate. Because the decision not to implement a particular OPSEC countermeasure entails risks, this step requires the commander's approval. Critical intelligence operations and sources may be compromised if OPSEC countermeasures are applied. Some operations and collection methods/sources may be too important to be compromised if the adversary detects friendly OPSEC countermeasures.

(2) Typical questions that might be asked when making this analysis include the following:

(a) What effect is likely to occur if a particular OPSEC countermeasure is implemented?

(b) What impact to mission success is likely to occur if an OPSEC countermeasure is not implemented?

(c) What impact to mission success is likely if an OPSEC countermeasure fails to be effective?

(d) What additional indicators may be collected by the adversary if an OPSEC countermeasure is implemented?

(3) **The interaction of OPSEC countermeasures should also be analyzed.** In some situations, certain OPSEC countermeasures may actually create indicators of critical information. For example, camouflaging previously unprotected facilities can indicate preparations for military action.

d. **The selection of measures must be coordinated with other capabilities of IO.** Actions such as jamming of intelligence nets or the physical destruction of critical intelligence centers can be used as OPSEC countermeasures. Conversely, MILDEC and military information support operations plans may require that OPSEC countermeasures not be applied to certain indicators in order to project a specific message to the adversary.

For more detailed discussion on risk assessment, see DOD 5205.02-M, DOD Operations Security (OPSEC) Program Manual.

6. Apply Operations Security Countermeasures

a. The command **implements the OPSEC countermeasures** selected in the risk assessment process or, in the case of planned future operations and activities, includes the measures in specific operations plans. Before OPSEC countermeasures can be selected, security objectives and critical information must be known, indicators identified, vulnerabilities assessed, and risks assessed.

A key action during the operations security process is to analyze potential vulnerabilities to joint forces. It requires identifying any operations security indicators that could reveal critical information about the operation, such as increased troop movement.

b. A general OPSEC countermeasure strategy should be to:

(1) Minimize predictability from previous operations.

(2) Determine detection indicators and protect them by elimination, control, or deception.

(3) Conceal indicators of key capabilities and potential objectives.

(4) Counter the inherent vulnerabilities in the execution of mission processes and the technologies used to support them.

c. During the execution of OPSEC countermeasures, OPSEC personnel should establish measures of effectiveness (MOEs) and measures of performance (MOPs) to assess if their OPSEC analysis is correct.

(1) MOE. **The adversary's reaction is monitored to determine the countermeasures' effectiveness and to provide feedback.** As it has been indicated above, implementing OPSEC countermeasures should not reveal additional critical information. As a corollary to that, if an OPSEC countermeasure is identified by the adversary, that, in itself, may be enough to alert the adversary that a military operation is imminent.

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

(3) Commanders and their staffs can use feedback to adjust ongoing activities and for future OPSEC planning. Provisions for feedback must be coordinated with the command's intelligence and CI staffs to ensure requirements that support OPSEC receive the appropriate priority. In addition to intelligence sources providing feedback, OPSEC assessments can provide useful information relating to the success of OPSEC countermeasures.

CHAPTER III
OPERATIONS SECURITY PLANNING

"Public Source: Using this public source openly and without resorting to illegal means, it is possible to gather at least 80% of information about the enemy. The percentage varies depending on the governments policy on freedom of the press and publication."

Manchester Document
Found on a Suspected Terrorist Computer During a
Police Raid in Manchester, England, 10 May 2000

1. General

a. Many nations and organizations, including violent extremist organizations, are actively engaged in conducting intelligence operations against the US and its armed forces. Open-source material and observations of US activities and operations are major sources of information for the adversary.

b. In order to prevent adversaries (or potential adversaries) from gaining critical information concerning friendly operations, joint forces must plan and execute OPSEC. To be effective, OPSEC must be considered as early as possible during mission planning and appropriately revised to keep pace with any changes in current operations and adversarial threats.

c. OPSEC planning and execution occur as part of the command's or organization's IO campaign. The commander's objectives are the basis for OPSEC planning.

2. Operations Security Factors

The following factors must be considered when conducting OPSEC planning:

a. **The commander plays a critical role in OPSEC planning.** OPSEC planning guidance should be provided as part of the commander's planning guidance. This allows OPSEC to be considered during the development of friendly COAs.

b. **OPSEC is an operations function, not a security function.** The OPSEC process is applied throughout the planning process and is performed by all planners, but especially the plans directorate of a joint staff and the J-3 operations planners. The planners are assisted by the organization's OPSEC program manager and appropriate planners from other staff elements. Intelligence support, as early as possible in the planning process, is particularly important in determining the threat to friendly operations, assessing friendly vulnerabilities, determining the adversary's capabilities, and predicting the adversary's COAs.

c. **OPSEC should be integrated into the IO cell.** The JFC's staff, which includes the IO cell, develops and promulgates guidance and plans for IO that are passed to the components and supporting organizations and agencies for detailed planning and execution.

While planning joint operations, including those requiring highly visible deployments, operations security must be considered as early as possible to prevent adversaries from gaining valuable intelligence.

The role of the OPSEC program manager is to facilitate OPSEC within the commander's plan. The OPSEC program manager coordinates combatant command or subordinate joint force OPSEC activities and coordinates with the communications systems directorate and other command organizations as necessary for NSA's joint COMSEC monitoring activity liaison. Close coordination between the MILDEC and OPSEC offices is critical as MILDEC and OPSEC can be mutually supportive when properly coordinated, but may be diametrically opposing when not properly coordinated.

d. **OPSEC planning should focus on identifying and protecting critical information.** Attempting to deny all information about a friendly operation or activity is seldom cost-effective or realistic. The OPSEC program focuses on the key pieces of information that need to be protected.

e. **The ultimate goal of OPSEC is increased mission effectiveness.** By preventing an adversary from determining friendly intentions or capabilities, OPSEC reduces losses to friendly units and increases the likelihood of achieving mission success.

f. **OPSEC is considered during the development and selection of friendly COAs.** COAs will differ in terms of how many OPSEC indicators will be created and how easily those indicators can be managed by OPSEC countermeasures. Depending upon how important maintaining secrecy is to mission success, OPSEC considerations may be a factor in selecting a COA.

g. **OPSEC planning is a continuous process.** During all phases of an operation, feedback on the success or failure of OPSEC countermeasures is evaluated based on MOEs, and the OPSEC plan is modified accordingly. Friendly intelligence and CI organizations, COMSEC monitoring, and OPSEC assessments are the primary sources for feedback information and are continuous throughout the OPSEC planning process.

h. **Apply OPSEC to the planning process.** Ensure that the critical information directly related to the actual planning process is protected to preclude providing indicators that tip off the operation being planned.

i. **The public affairs officer (PAO) participates in OPSEC planning** to provide assessments on the possible effects of media coverage and all other public release of information by members of the command. PA planning should include considerations to reduce the time lag between an event and what can be communicated as well as the coordination of OPSEC countermeasures and PA ground rules. The PAO ensures that the media pool, media clearances, media releases, and authorization of video transmissions are within the established OPSEC countermeasures. The PAO also coordinates with the OPSEC program manager to ensure the command (internal) information program addresses OPSEC and ground rules for the release of information (officially or unofficially) by military members through the Internet and other communications mediums subject to public access or monitoring.

See JP 3-61, Public Affairs, *for further details.*

j. **OPSEC is an inherent part of** the integration, coordination, deconfliction, and synchronization of **all multinational information activities** within the JFC's operational area.

k. **The termination of OPSEC countermeasures must be addressed in the OPSEC plan** to prevent future adversaries from developing countermeasures to successful OPSEC countermeasures. The OPSEC plan should provide guidance on how to prevent the target of the execution operations, as well as any interested third parties, from discovering critical information relating to OPSEC during the post-execution phase.

3. Operations Security Indicators

a. OPSEC indicators are friendly detectable actions and open-source information that can be interpreted or pieced together by an adversary to derive critical information. These indicators must be continuously analyzed and considered during planning.

b. **Basic Operations Security Indicator Characteristics.** An indicator's characteristics are elements of an action or piece of information that are potentially useful to an adversary. There are five major characteristics:

(1) Signature

(a) A signature is the characteristic of an indicator that makes it identifiable or causes it to stand out. Key signature properties are uniqueness and stability. Uncommon or

unique features reduce the ambiguity of an indicator and minimize the number of other indicators that must be observed to confirm a single indicator's significance.

(b) An indicator's signature stability, implying constant or stereotyped behavior, can allow an adversary to anticipate future actions. Varying the pattern of behavior decreases the signature's stability and thus increases the ambiguity of the adversary's observations.

(c) Procedural features are an important part of any indicator signature and may provide the greatest value to an adversary. They identify how, when, and where the indicator occurs and what part it plays in the overall scheme of operations and activities.

(2) Associations

(a) Association is the relationship of an indicator to other information or activities. It is an important key to an adversary's interpretation of ongoing activity. Intelligence analysts continually compare their current observations with what has been seen in the past in an effort to identify possible relationships. For example, a distinctive piece of ground-support equipment known to be used for servicing strategic bombers might be observed at a tactical fighter base. An intelligence analyst could conclude that a strategic bomber presence has been or will be established there. The analyst will then look for other indicators associated with bombers to verify that conclusion.

(b) Another key association deals with continuity of actions, objects, or other indicators that may register as patterns to the observer or analyst. Such continuity may not be the result of planned procedures but may result instead from repetitive practices or sequencing to accomplish a goal. If, for example, the intensive generation of aircraft sorties is always preceded by a maintenance standdown to increase aircraft readiness, detecting and observing the standdown may allow the adversary analyst or observer to predict the subsequent launch activity. Moreover, based on past patterns of the length of such standdowns, the analyst may be able to judge the scope of the sortie generation.

(c) Another type of association that is useful to intelligence analysts is organizational patterns. Military units, for example, are often symmetrically organized. Thus, when some components are detected, others that are not readily apparent can be assumed to exist. For example, an intelligence analyst knows that a particular army's infantry battalions are organized with three infantry companies, a headquarters company, and a weapons company. If only the headquarters company and one infantry company are currently being detected, the presence of the other known battalion components will be strongly suspected. Thus in some situations, a pattern taken as a whole can be treated as a single indicator, simplifying the intelligence problem.

(3) Profiles

(a) Each functional activity generates its own set of more-or-less unique signatures and associations. The sum of these signatures and associations is the activity's profile. An activity's profile is usually unique. Given enough data, intelligence analysts can

determine the profile of any activity. Most intelligence organizations seek to identify and record the profiles of their adversary's military activities and human factors.

(b) The profile of an aircraft deployment, for example, may be unique to the aircraft type or mission. This profile, in turn, has several subprofiles for the functional activities needed to deploy the particular mission aircraft (e.g., fuels, avionics, munitions, communications, air traffic control, supply, personnel, and transportation).

(c) The observation of a unique profile may sometimes be the only key that an intelligence analyst needs to determine what type of operation is occurring, thus minimizing the need to look harder for additional clues. Such unique profiles cut the time needed to make accurate intelligence estimates. As a result, profiles are the analytical tools.

(d) The profile and analysis of a particular decision maker may predict the outcome of an aircraft deployment. Decision makers can react differently because of societal pressures, group dynamics, cultures, personal experiences, and governments.

(4) Contrasts

(a) Contrasts are any differences that are observed between an activity's standard profile and its most recent or current actions. Contrasts are the most reliable means of detection because they depend on changes to established profiles. They also are simpler to use because they need only to be recognized, not understood.

(b) Deviations from normal profiles will normally attract the interest of intelligence analysts. They will want to know why there is a change and attempt to determine if the change means anything significant.

(c) In the previous example of the distinctive bomber-associated ground support equipment at a fighter base, the intelligence observer might ask the following questions:

1. Have bombers been deployed at fighter bases before? At this particular fighter base? At several fighter bases simultaneously?

2. If there have been previous bomber deployments, were they routine or did they occur during some period of crisis?

3. If previous deployments have been made to this base or other fighter bases, how many bomber aircraft were deployed?

4. What actions occurred while the bombers were deployed at the fighter bases?

5. What is happening at other fighter and bomber bases? Is this an isolated incident or one of many changes to normal activity patterns?

6. Who will decide where, when, what, and how fighter bombers will deploy?

(d) Although the detection of a single contrast may not provide intelligence analysts with a total understanding of what is happening, it may result in increased intelligence collection efforts against an activity or human target.

(5) Exposure

(a) Exposure refers to when and for how long an indicator is observed. The duration, repetition, and timing of an indicator's exposure can affect its relative importance and meaning. Limiting the duration and repetition of exposure reduces the amount of detail that can be observed and the associations that can be formed.

(b) An indicator (object or action) that appears over a long period of time will be assimilated into an overall profile and assigned a meaning. An indicator that appears for a short time and does not appear again may, if it has a high interest value, persist in the adversary intelligence database or, if there is little or no interest, fade into the background of insignificant anomalies. An indicator that appears repeatedly will be studied carefully as a contrast to normal profiles.

(c) Because of a short exposure time, the observer or analyst may not detect key characteristics of the indicator the first time it is seen, but can formulate questions and focus collection assets to provide answers if the indicator is observed again.

(d) Repetition of the indicator in relationship to an operation, activity, or exercise will add it to the profile even if the purpose of the indicator is not understood by the adversary. Indicators limited to a single isolated exposure are difficult to detect and evaluate.

4. Operations Security Countermeasures

a. **Introduction.** The following OPSEC countermeasures are offered as a guide only. Development of specific OPSEC countermeasures is as varied as the specific vulnerabilities they are designed to offset.

b. **Operational and Logistic Measures**

(1) Randomize the performance of functions and operational missions. Avoid repetitive or stereotyped tactics and procedures for executing operations or activities in terms of time, place, event sequencing, formations, and command and control (C2) arrangements.

(2) Employ force dispositions and C2 arrangements that conceal the location, identity, and command relationships of major units.

(3) Conduct support activities in a way that will not reveal intensification of preparations before initiating operations.

(4) Transport supplies and personnel to combat units in a way that conceals the location and identity of the combat units.

(5) Operate aircraft at low altitude to avoid radar detection.

(6) Operate to minimize the reflective surfaces that units or weapon systems present to radars and sonars.

(7) Use darkness to mask deployments or force generation.

(8) Approach an objective "out of the sun" to prevent detection.

(9) Physical Attack and Electronic Warfare. During hostilities, use physical destruction and electronic attack against the adversary's ability to collect and process information. Military actions that are used in support of OPSEC include strikes against an adversary's satellites, SIGINT sites, radars, fixed sonar installations, reconnaissance aircraft, and ships. For more information, see JP 3-13.1, *Electronic Warfare*, and JP 3-60, *Joint Targeting.*

c. **Technical Measures**

(1) Limit nonsecure computer e-mail messages to nonmilitary activities. Do not provide operational information in nonsecure e-mail messages.

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

(3) Use encryption to protect voice, data, and video communications.

(4) Use radio communications emission control, low-probability-of-intercept techniques and systems, traffic flow security, padding, flashing light or flag hoist, ultra-high-frequency relay via aircraft, burst transmission technologies, secure phones, landlines, and couriers. Limit use of high-frequency radios and directional super-high-frequency transponders.

(5) Control radar emission, operate at reduced power, operate radars common to many units, assign radar guard to units detached from formations or to air early warning aircraft, and use anechoic coatings.

(6) Mask emissions or forces from radar or visual detection by use of terrain (such as mountains and islands).

(7) Maintain sound silence or operate at reduced power, proceed at slow speeds, turn off selected equipment, and use anechoic coatings.

(8) Use screen jamming, camouflage, smoke, background noise, added sources of heat or light, paint, or weather.

d. **Administrative Measures**

(1) Limit nonsecure telephone conversation with nonmilitary activities.

(2) Avoid bulletin board, plan of the day, or planning schedule notices that reveal when events will occur.

(3) Conceal budgetary transactions, supply requests and actions, and arrangements for services that reveal preparations for activity.

(4) Conceal the issuance of orders, the movement of specially qualified personnel to units, and the installation of special capabilities.

(5) Control trash and garbage dumping or other housekeeping functions to conceal the locations and identities of units.

(6) Follow normal leave and liberty policies to the maximum extent possible before an operation starts in order to preserve a sense of normalcy.

(7) Ensure that personnel discretely prepare for their families' welfare in their absence and that their families are sensitized to a potentially abrupt departure.

(8) Provide family OPSEC briefs to inform family members of the need for OPSEC.

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

(10) Ensure that adequate policy and procedures are in place for shredding documents.

e. **Operations Security and Military Deception**

(1) OPSEC used in conjunction with MILDEC can assist commanders in protecting key elements of operations and facilitate mission success. OPSEC, with MILDEC, can be used to:

(a) Cause adversary intelligence to fail to target friendly activity; collect against targeted tests, operations, exercises, or other activities; or determine through analysis vital capabilities and characteristics of systems and vital aspects of policies, procedures, doctrine, and tactics.

(b) Create confusion about, or multiple interpretations of, vital information obtainable from open sources.

(c) Cause a loss of interest by foreign and random observers in test, operation, exercise, or other activity.

(d) Convey inaccurate locating and targeting information to opposing forces.

(2) In accordance with DOD policy, commanders are authorized to conduct MILDEC:

(a) To support OPSEC during the preparation and execution phases of normal operations, provided that prior coordination is accomplished for actions that will affect other commanders.

(b) When the commander's forces are engaged or are subject to imminent attack.

5. Planning Coordination

a. **General.** OPSEC coordination is continuous across all phases of an operation and the range of military operations and at every level of war. OPSEC planning is integrated with post-conflict activities, which may be transitioned to a foreign military or government, nongovernmental organizations (NGOs), or intergovernmental peacekeeping forces.

b. **Joint Planning Group.** JFCs normally establish a joint planning group (JPG). Early and continuous exchange of information and close coordination of planning activities between the JPG and the OPSEC representative are essential to successful integration of OPSEC into planning and execution. JPG members should also have OPSEC training.

c. **OPSEC Planning.** OPSEC planning in support of joint operations is accomplished through the application of the OPSEC process. The five actions that compose the OPSEC process are described in detail in Chapter II, "The Operations Security Process." OPSEC planning is always done in conjunction with joint operation planning and is a part of the overall IO planning effort.

d. **OPSEC and the Deliberate Planning Process.** When OPSEC planning is being conducted below the combatant command level, clear, two-way communications must be established to ensure the chain of command is fully apprised of all OPSEC contingency planning activities that may require synchronization, coordination, or deconfliction. Deliberate planning is planning conducted in anticipation of a situation that might involve military forces and is normally conducted through a deliberate, detailed process. The OPSEC process must be applied to this planning process to ensure that critical information is protected. To do so, the OPSEC program manager must be fully integrated into all facets of the planning process as well as the review of existing contingency plans.

e. **OPSEC and the Crisis Action Planning Process.** In contrast to deliberate planning, crisis action planning normally takes place in a compressed time period. Coordination of the OPSEC plan is even more crucial in crisis action planning than in deliberate planning. Even with a compressed timeframe, the OPSEC program manager must ensure that the OPSEC process is conducted to ensure that critical information is not compromised.

See JP 5-0, Joint Operation Planning, *for further guidance.*

6. Joint and Interagency Planning

a. The OPSEC process is an inherent part of the whole-of-government approach to operations. National Security Decision Directive 298, *National Operations Security Program,* mandates the establishment of formal OPSEC programs for all executive departments or agencies that support national security missions. The current operational environment may require coordination of OPSEC efforts with other government departments and agencies, such as the Central Intelligence Agency, Department of Homeland Security, Department of Energy, or Federal Bureau of Investigation.

b. **Joint Interagency Coordination Group (JIACG).** When formed at a combatant command, the JIACG provides a venue for integrating other government departments and agencies into joint operation planning. The IO cell within the joint staff will need to coordinate OPSEC planning efforts with the JIACG throughout the joint operation planning process.

c. Military planners should include interagency partners when developing the CIL and pay particular attention to avoid creating additional OPSEC vulnerabilities while coordinating with other US Government departments and agencies that are not controlled by the JFC. Military planners also need to include other US Government department and agency activities in the assessment process, along with those of the component forces.

For further information on joint and interagency planning, see JP 3-08, Interorganizational Coordination During Joint Operations.

7. Multinational Planning

a. US military operations often are conducted with the armed forces of other nations in pursuit of common objectives. Multinational operations, both those that include combat and those that do not, are conducted within the structure of an alliance or coalition. Further, some multinational activities are conducted with partner nations that are not part of an alliance or coalition.

b. Multinational operations and activities require close cooperation among all forces and can serve to mass strengths, reduce vulnerabilities, and provide legitimacy. OPSEC countermeasures that apply to joint operations are also appropriate for multinational situations.

c. Plans should be issued far enough in advance to allow sufficient time for member forces to conduct their own planning and rehearsals. Some non-US forces may not have the planning and execution agility and flexibility characteristic of US forces. Accordingly, JFCs should ensure that the tempo of planning and execution does not exceed their capabilities.

d. Intelligence. The collection, production, and dissemination of intelligence can be a major challenge. Multinational force members normally operate separate intelligence systems in support of their own policy and military forces. JFCs should establish a system

that optimizes each nation's contributions and provides member forces a common intelligence picture, tailored to their requirements and consistent with disclosure policies of member nations.

(1) JFCs, in accordance with national directives, need to determine what intelligence may be shared with other nations' forces early in the planning process. The limits of intelligence sharing and the procedures for doing so should be included in agreements with multinational partners that are concluded after obtaining proper authorization.

(2) The National Disclosure Policy provides guidance. It promulgates national policy and procedures in the form of specific disclosure criteria and limitations, definitions of terms, release arrangements, and other guidance. It also establishes interagency mechanisms and procedures for the effective implementation of the policy. In the absence of sufficient guidance, JFCs should share only information that is mission-essential, affects lower-level operations, facilitates combat identification, and is perishable.

For further information, see JP 3-16, Multinational Operations.

8. Intergovernmental and Nongovernmental Organization Considerations

a. Intergovernmental organizations (IGOs) and NGOs are prominent participants in the current operating environment, particularly in foreign humanitarian assistance, peace, and stability operations. IGOs and NGOs provide a wide range of capabilities that are not controlled by JFC, but their presence in the operational area must be accounted for during joint operation and OPSEC planning. JFCs normally interact with IGOs and NGOs through a civil-military operations center (CMOC) or a joint civil-military operations task force (JCMOTF). Military planners must be aware of the differences in these organizations.

(1) **IGOs** are organizations created by a formal agreement (e.g., a treaty) between two or more governments. They may be established on a global, regional, or functional basis for wide-ranging or narrowly defined purposes. They are formed to protect and promote national interests shared by member states. Examples include the United Nations, North Atlantic Treaty Organization, and African Union. Most are some sort of security organization, bound together for mutual protection. Some are general in nature and, for instance, are bound for economic reasons such as the Economic Community of West African States. Some have both functions. IGOs have defined structures, roles, and responsibilities. Their ability to participate in joint operation and OPSEC coordination depends on their resources and the expertise they can bring to a problem.

(2) **NGOs** are private, self-governing, not-for-profit organizations dedicated to alleviating human suffering; promoting education, health care, economic development, environmental protection, human rights, and conflict resolution; or encouraging the establishment of democratic institutions and civil society. They can have any form or structure, and are independent, diverse, and usually grassroots focused. They are primarily in the business of providing relief and assistance during unusual situations. In the event of a long-term problem, they will most likely be on-scene and active well before the US military

gets invited in. NGOs are willing to work in high-risk situations and will likely be in the area long after the military has departed. Like IGOs, NGOs vary in size from very large, (e.g., International Red Cross), to very small local organizations dedicated to a particular emergency or disaster. Budgets and experience levels also vary greatly. NGOs can be expected to be present in nearly every situation in which the US military might be called to serve. Some NGOs operating in the area may not be friendly to US or partner nations and could actually collect information and pass on to our adversaries. Care should be taken when working with these NGOs.

b. **Military planners must consider and assess potential OPSEC vulnerabilities and threats whenever IGOs and NGOs are present in the operational area.** Joint force representatives in the CMOC or JCMOTF must be vigilant in protecting critical information when coordinating with various IGOs and NGOs. While IGOs and NGOs provide unique capabilities, they may also create a large vulnerability for the loss of critical information. In many cases, IGOs and NGOs will have established relationships with US Government departments and agencies such as the US Department of State. Another significant vulnerability of many NGOs is their reliance on nonsecure communications, such as free e-mail accounts and social networking sites, for the conduct of routine operations. Commanders at all levels need to balance the need to share information with these partner organizations with the realization that once shared, the information may be available for collection. Military planners must ensure that all of these relationships are included in developing the CIL, identifying OPSEC indicators, and applying OPSEC countermeasures.

c. **Integration.** It is vital to integrate IGOs and NGOs into joint operation planning as early as possible so that an integrated and achievable OPSEC strategy can be developed. Initial requirements for integrations include clarification of objectives; understanding how partners intend to conduct activities; establishment of liaison and deconfliction procedures; and identification of vulnerabilities and possible countermeasures to adversary exploitation. Whether planning is based on APEX or on established foreign or alliance planning processes, planners must recognize the differing institutional cultural values, interests and concerns, moral and ethical values, rules of engagement, and legal constraints and allow for complications in planning and execution in multiple languages.

THE "BLACK HOLE": OPSEC DURING PLANNING

During the autumn of 1990, joint force air component commander (JFACC) planners merged the Air Force Component, Central Command (CENTAF) predeployment concept of operations with the INSTANT THUNDER concept to form the foundation for the Operation DESERT STORM plan for air operations.

US Navy, US Marine Corps (USMC), and US Army planners worked closely with US Air Force (USAF) planners in August and September to draft the initial offensive air plan. In Riyadh, Navy Component, Central Command, Marine Corps Component, Central Command, and Army Component, Central Command were integral planning process members. Royal Air Force (RAF) planners joined the JFACC staff on 19 September.

US Central Command's offensive air special planning group, in the Royal Saudi Air Force headquarters, was part of the JFACC staff and eventually became known as the "Black Hole" because of the extreme secrecy surrounding its activities. The Black Hole was led by a USAF brigadier general, reassigned from the *USS Lasalle,* where he had been serving as the deputy commander of Joint Task Force Middle East when Iraq invaded Kuwait. His small staff grew gradually to about 30 and included RAF, Army, Navy, USMC, and USAF personnel. By 15 September, the initial air planning stage was complete; the President was advised that there were sufficient air forces to execute and sustain an offensive strategic air attack against Iraq, should he order one. However, because of operations security concerns, most of CENTAF headquarters was denied information on the plan until only a few hours before execution.

SOURCE: Final Report to Congress
Conduct of the Persian Gulf War, April 1992

Intentionally Blank

CHAPTER IV
OPERATIONS SECURITY ASSESSMENTS

"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."

George Washington

1. Assessments and Surveys

a. **General.** An OPSEC assessment is an intensive application of the OPSEC process to an existing operation or activity. Assessments are essential for identifying requirements for additional OPSEC countermeasures and for making necessary changes in existing plans. An OPSEC assessment is a good tool to validate OPSEC programs and organizational practices to protect critical information in operations. In addition to using organic assets to conduct assessments, JFCs can seek the support of external resources. An OPSEC survey is conducted by a team of external subject matter experts from multiple disciplines to simulate adversary intelligence processes.

b. **Purpose.** The purpose of an OPSEC assessment is to thoroughly examine an operation or activity to determine if adequate protection from adversary intelligence exploitation exists. Ideally, the operation or activity being assessed uses OPSEC countermeasures to protect its critical information. The OPSEC assessment is used to verify the effectiveness of OPSEC countermeasures. The assessment will determine if critical information identified during the OPSEC planning process is being protected. An assessment cannot be conducted until after an operation or activity has at least identified its critical information. Without a basis of critical information, there can be no specific determination that actual OPSEC vulnerabilities exist. The purpose of an OPSEC survey is to focus on the organization's ability to adequately protect critical information from adversary intelligence exploitation during planning, preparation, execution, and postexecution phases of any operation or program.

c. **Uniqueness**

(1) Each OPSEC assessment is unique. Assessments differ in the nature of the information requiring protection, the adversary collection capability, and the environment of the activity to be assessed.

(2) In combat, an assessment's emphasis should be on identifying vulnerabilities and indicators that signal friendly intentions, capabilities, and limitations and that permit the adversary to counter friendly operations or reduce their effectiveness.

(3) During noncombat operations, to include routine steady-state activities, assessments generally seek to correct weaknesses that disclose information useful to potential adversaries in the event of future conflict. Many activities, such as operational unit

tests, drills, practice alerts, and major exercises, are of great interest to a potential adversary because they provide insight into friendly readiness, plans, crisis procedures, and C2 capabilities that enhance that adversary's planning.

d. **Operations Security Assessments Versus Security Inspections**

(1) OPSEC assessments are different from security evaluations or inspections. An assessment attempts to produce an adversary's view of the operation or activity being assessed. A security inspection seeks to determine if an organization is in compliance with the appropriate security directives and regulations.

(2) Assessments are always planned and conducted by the organization responsible for the operation or activity that is to be assessed. Inspections may be conducted without warning by outside organizations.

(3) OPSEC assessments are not a check on the effectiveness of an organization's security programs or its adherence to security directives. In fact, assessment teams will be seeking to determine if any security measures are creating OPSEC indicators.

(4) Assessments are not punitive inspections, and no grades or evaluations are awarded as a result of them. Assessments are not designed to inspect individuals, but are employed to evaluate operations and systems used to accomplish missions.

(5) To obtain accurate information, an assessment team should try to create an environment that promotes positive cooperation and assistance from the organizations participating in the operation or activity being assessed. If team members must question individuals, observe activities, and otherwise gather data during the course of the assessment, they will inevitably appear as inspectors, unless this nonpunitive objective is made clear.

(6) Although reports are not provided to the assessed unit's higher headquarters, OPSEC assessment teams may forward to senior officials the lessons learned on a nonattribution basis. The senior officials responsible for the operation or activity then decide to further disseminate the assessment's lessons learned.

(7) Lessons learned from the assessment should be shared with command personnel in order to improve the command's OPSEC posture and mission effectiveness.

e. **Assessments and Surveys**

(1) **OPSEC Assessment.** OPSEC assessments are conducted annually to evaluate an operation, activity, exercise, or support function to determine the likelihood that critical information can be protected from the adversary's intelligence collection systems. An OPSEC assessment is normally run by the OPSEC program manager and performed by the unit's OPSEC working group. An assessment may be conducted with a small team of individuals from within an organization with or without assistance from subject matter experts. The scope of an OPSEC assessment is usually limited to events and/or activities within that organization.

(2) **OPSEC Survey.** A survey usually requires a team of external subject matter experts from multiple disciplines to simulate adversary intelligence processes. An OPSEC survey should focus on the organization's ability to adequately protect critical information from adversary intelligence exploitation during planning, preparation, execution, and post-execution phases of any operation or program. These surveys may include telecommunications monitoring, radio frequency monitoring, network and computer systems assessment, and open-source collection. Survey teams should use collection techniques of known adversaries. A survey is required every three years. See Figure IV-1 for an assessment–survey comparison.

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

Figure IV-1. Assessment–Survey Comparison

2. Assessment Planning

a. **Introduction.** The required lead time to prepare for an assessment depends on the nature and complexity of the operation and activities assessed (combat operations, peacetime operational activity, or other type of operation). Allot sufficient time in the planning phase for a thorough review of pertinent documentation, for formal and informal coordination and discussions, and for careful preparation of functional outlines. The following actions normally make up the planning phase.

b. **Determine the Scope of the Assessment.** The scope of the assessment is defined at the start of the planning phase and limited to manageable proportions. Limitations are imposed by geography, time, units to be observed, funding, and other practical matters.

c. **Select Team Members**

(1) Regardless of the assessment's external or internal focus, the team should contain multidisciplined expertise. Assessment team members should be selected for their analytical, observational, and problem-solving abilities.

(2) Since assessments are normally oriented to operations, the senior member should be selected from the operations (or equivalent) staff of the commander responsible for conducting the assessment.

(3) Typical team members would represent the functional areas of intelligence (to include CI), security, communications, logistics, plans, IA, PA, contracting, acquisition, and administration. When appropriate, specialists from other functional areas, such as transportation, will participate. Team members are brought together early in the planning phase to ensure timely, thorough accomplishment of the tasks outlined below.

d. **Become Familiar with Assessment Procedures.** Designating team members with assessment experience is advantageous, but is often not possible. In such cases, team members will require familiarization with assessment procedures. Refer to DOD 5205.02-M, *DOD Operations Security (OPSEC) Program Manual*, Enclosure 4, for more information.

e. **Analyze the Adversary Intelligence Threat.** Because assessments are conducted from an adversarial perspective, it is important to conduct a comprehensive all-source threat assessment that addresses any updates to the adversary intelligence capability.

f. **Understand the Operation or Activity Assessed.** The team members' thorough understanding of the operation or activity to be assessed is crucial to ensuring the success of subsequent phases of the assessment. Team members should become familiar with the OPLANs, OPORDs, MILDEC activities, standard operating procedures (SOPs), or other directives bearing on the assessed operation or activity. This initial review familiarizes team members with the mission and concept of operations and identifies most of the organizations participating in the assessed activity (others may be identified as the assessment progresses).

g. **Review Empirical Studies.** Empirical studies, such as communications monitoring or CI reports, simulate aspects of the adversary intelligence threat and support vulnerability findings. These studies also help the assessment team identify vulnerabilities that cannot be determined through interviews and observation. The results of these studies are useful to the assessment team during the field or analytic phase of the assessment. Arrangements for their use should be made as far in advance of the assessment as possible.

h. **Develop a Functional Outline**

(1) A basic OPSEC assessment technique involves the construction of a chronology of events that are expected to occur in the assessed operation or activity. Events are assembled sequentially, thus creating a timeline that describes in detail the activities or plans of an operation or activity.

(2) After the chronology is assembled, vulnerabilities can be identified in light of the known or projected threat. (see examples at Appendix B, "Functional Outlines and Profiles"). Collectively, the outlines project a time-phased picture of the events associated with the planning, preparation, execution, and conclusion of the operation or activity. The outlines also provide an analytic basis for identifying events and activities that are vulnerable to adversary exploitation.

i. **Determine Preliminary Friendly Vulnerabilities.** After the adversary intelligence threat and the OPSEC indicators are determined, a subjective evaluation must be made of the potential friendly vulnerabilities. A vulnerability (e.g., a detectable, exploitable event) may or may not carry a security classification at the time of its identification, but such preliminary vulnerabilities must be protected from disclosure by administrative or security controls. These preliminary friendly vulnerabilities are refined in later stages of the OPSEC assessment.

j. **Announce the Assessment**

(1) After team members are selected and are familiar with the operation or activity to be assessed, the organization conducting the assessment should inform its subordinate and supporting organizations that an assessment will be conducted so that preparations can be made to support the team during the field assessment phase.

(2) The following information should be included:

(a) Assessment purpose and scope.

(b) List of team members and their clearances.

(c) List of required briefings and orientations.

(d) Timeframe involved.

(e) Administrative support requirements.

(f) All support requirements, such as COMSEC monitoring support requirements (if needed).

(g) Network vulnerability assessments requirements (as needed).

3. Assessment Execution

a. **Introduction.** As noted previously, data collection begins in the planning phase with a review of associated documentation. During the assessment phase, interviews with personnel directly involved in the operation, together with observations and document collection, are the primary means of data collection. The following actions are normally accomplished during the assessment phase.

b. **Command Briefing on Operation to Be Assessed.** This briefing is presented to the OPSEC assessment team by the command directing the forces or assets involved in the operation or activity being assessed. The purpose of the briefing is to provide the assessment team with an overview of the operation from the command's point of view. Team members should use this opportunity to clarify remaining questions about the information developed in the planning phase.

c. **Operations Security Assessment Team Briefing.** This briefing is presented by the chief of the assessment team to the commander and principal staff officers of the assessed organization. The briefing may be either a formal presentation or an informal discussion. The objective is to inform the commander and the staff of how the assessment will be conducted. The briefing includes a summary of the relevant threat and the vulnerability assessment developed during the planning phase. The staff should be asked to comment on the validity of this assessment. Results of previous OPSEC assessments of similar activities may be summarized.

d. **Data Collection and Functional Outline Refinement**

(1) During the assessment phase, data is collected through observation of activities, document collection, and personnel interviews. Data may also be acquired through concurrent ongoing empirical data collection, such as COMSEC monitoring.

(2) Team members must be alert to differences between what they have read, what they have assumed to be the situation, what they have been told in the command briefing, and what they observe and are told by personnel participating in the operation. Conflicting data are to be expected.

(3) While observations can verify the occurrence, sequence, and exact timing of events, much essential information must be gathered from interviews.

(a) Functional outlines should be reviewed before and after interviews to ensure that all pertinent points are covered. Specifics on how, when, and where people accomplish their tasks, and how these tasks relate to the planned and observed sequence of events, are recorded in order to document activities in a logical sequence.

(b) Team members should assure interviewees that all sources of information are protected by a nonattribution policy.

(c) Interviews are best conducted by two team members.

(d) Facts to be recorded during or soon after the interview normally include:

1. Identification and purpose of the interview.

2. Description of the billets occupied by the individuals being interviewed.

3. Details of exactly what tasks the individuals perform and how, when, and where they perform them with a view toward determining what information they receive, handle, or generate, and what they do with it.

4. Whether the individuals' actions reflect an awareness of a hostile intelligence collection threat.

(4) Tentative findings will begin to emerge as data collection proceeds and information is reviewed and compared. The findings should be confirmed and fully documented as quickly as possible.

(5) If a finding is considered to have serious mission impact, it should be made known to the commander responsible for the operation in order to permit early corrective actions.

(6) Development of findings during the assessment phase ensures access to supporting data and precludes the need to reconstruct evidence after the team has left the scene. Following this procedure, the basic findings and supporting data of the final assessment report are well developed before the end of the assessment phase. Final development and production of the assessment report can then proceed immediately upon the team's return to home station.

e. **Team Employment**

(1) The complexity, size, and duration of the assessed operation or activity will determine the general employment of the assessment team. Tentative locations for data collection, developed during the planning phase, provide initial indications of how and where to employ the team.

(2) It is rarely possible, however, to plan employment in detail before the assessment phase. A limited, short duration operation with few participating elements may permit concentrating the team in one, or a very few, locations. Larger and longer operations may require complete dispersal of the team, movement of the entire team from one location to another, or both, over a substantial period of time. The most reliable guideline for the team chief in determining how to employ the team is to reassemble it daily, either physically or via a collaborative method, to assess progress, compare data, and coordinate the direction of the assessment.

(3) The duration of the assessment phase is established during the planning phase and depends on how rapidly data is collected. Many assessments have required 30 days or more. Less comprehensive ones might require a week to 10 days. The proximity of data collection locations to each other, number of such locations, transportation availability, and degree of difficulty experienced in resolving conflicting data are some of the factors affecting duration of the assessment phase.

f. **Operations Security Assessment Team Exit Briefing**

(1) An exit briefing should be presented to the commander before the team leaves a command, regardless of previous reports or tentative findings. Like the entrance briefing, the exit briefing can be an informal discussion with the commander or a formal briefing for the commander and the staff.

(2) The tentative nature of assessment findings should be emphasized. Even those that appear to be firm may be altered by the final data review as the assessment report is prepared. Because preparation of the written report may take some time, the exit briefing can serve as an interim basis for further consideration and possible action by the commander.

(3) The distribution of the final written report should be clearly stated during the exit briefing. Normally, the report is provided directly to the commander. Some commands have found it useful to forward an interim report to the assessed commander for comments before proceeding with the final version.

4. Analysis and Reporting

During this portion, the OPSEC team correlates the data acquired by individual members with information from any empirical studies conducted in conjunction with the assessment.

a. **Correlation of Data**

(1) **Correlation of Functional Outlines.** When the separate chronology outlines for each functional area are correlated, the chronology of events for the operation or activity as a whole will emerge. Review and compare assessment data to clarify any conflicts.

(2) **Correlation of Empirical Data.** In addition to correlating data acquired from the observations of individual team members, the assessment team may also use relevant, empirically derived data to refine individual functional outlines. More important, this data can also verify vulnerabilities that would otherwise be exceedingly speculative or tenuous. Empirical data is extremely important to a comprehensive assessment.

b. **Identification of Vulnerabilities**

(1) The correlation and analysis of data help the team to refine previously identified preliminary vulnerabilities or isolate new ones. This analysis is accomplished in a manner similar to the way in which adversaries would process information through their intelligence systems.

(2) Indicators that are potentially observable are identified as vulnerabilities. Vulnerabilities point out situations that an adversary may be able to exploit. The key factors of a vulnerability are observable indicators, an intelligence collection threat to those indicators, and capability to impact friendly operations.

(3) The degree of risk to the friendly mission depends on the adversary's ability to react to the situation in sufficient time to degrade friendly mission or task effectiveness.

c. **Operations Security Assessment Report**

(1) The report of the OPSEC assessment is addressed to the commander of the assessed operation or activity. Lengthy reports (more than 15 pages) should be accompanied by an executive summary.

(2) The report should provide a discussion of identified critical information, indicators, adversaries and their intelligence capabilities, OPSEC vulnerabilities, risk analysis, and recommended OPSEC countermeasures to eliminate or reduce the vulnerabilities. Although some vulnerabilities may be virtually impossible to eliminate or reduce, they are included in the report to enable commanders to assess their operation or activity more realistically.

(3) Each report should contain a threat statement. Its length and classification need only be adequate to substantiate the vulnerabilities (or actual sources of adversary information) described in the report. The statement may be included in the main body of the report or as an annex. Portions of the threat that apply to a particular vulnerability finding are concisely stated as substantiation in a paragraph preceding or following the explanation of the observation. If the threat statement is so classified that it will impede the desired distribution and handling, the statement, or parts of it, should be affixed as an annex that is included only in copies of the assessment report provided to appropriately cleared recipients.

(4) The section that delineates vulnerabilities can be presented in a sequence that correlates with their significance, in an order that coincides with their appearance in the chronological progression of the assessed operation or activity, or grouped together according to functional area (logistics, communications, personnel). A particular vulnerability can be introduced by a headline followed by an adequate description of the finding and accompanied by identification of that portion of the operation or activity that includes the vulnerability. As stated earlier, a vulnerability observation may also include relevant threat references.

(5) If possible, OPSEC teams should include recommendations for corrective actions in the report. However, the team is not compelled to accompany each vulnerability finding with a recommendation. In some situations, the team may not be qualified to devise the corrective action; in others, it may not have an appreciation of the limitations in resources and options of a particular command. It may sometimes be more effective for the team to present the recommendation informally rather than including it in the assessment report. Recommendations of the OPSEC team may be particularly valuable in situations in which a vulnerability crosses command lines. Ultimately, commanders or the responsible officials

must assess the effect of possible adversary exploitation of vulnerabilities on the effectiveness of their operation or activity. They must then decide between implementing corrective actions or accepting the risk posed by the vulnerability.

(6) Appendixes and annexes to OPSEC assessment reports may be added to support the vulnerability findings and conclusions. Sections, such as a threat annex, may include empirical studies (or parts of them). Maps, diagrams, and other illustrative materials are some ways to substantiate OPSEC vulnerabilities.

(7) The report may end with a conclusion or summary of the assessment and its findings. The summary should not include judgments about compliance with standing security practices of the organizations. Such judgments are the purview of security disciplines.

(8) Distribution of the assessment team's report should be limited to the principal commands responsible for the assessed operation or activity. After the commands have had time to evaluate the report and take corrective actions, they can consider additional distribution. Abstracts from the report may be provided for lessons learned documents or databases on a nonattribution basis.

(9) Because they contain vulnerability information, OPSEC assessment reports must be controlled from release to unauthorized persons or agencies. Affected portions of the report are controlled in accordance with applicable security classification guides. For those portions of the report not controlled by security classification guides, administrative control of the release of assessment report information must be considered. Likewise, the notes, interviews, and raw data used to build an assessment report are subject to the same controls as the finished report.

APPENDIX A
OPERATIONS SECURITY INDICATORS

The following paragraphs provide examples of indicators that are associated with selected military activities and information. This list is not all-inclusive and is presented to stimulate thinking about what kinds of actions can convey indicators that betray critical information for specific friendly operations or activities.

1. Indicators of General Military Force Capabilities

a. The presence of unusual type units for a given location, area, or base.

b. Friendly reactions to adversary exercises or actual hostile actions.

c. Actions, information, or material associating Reserve Component units or forces with specific commands or units (e.g., mobilization and assignment of reserve personnel to units).

d. Actions, information, or material indicating the levels of unit manning as well as the state of training and experience of personnel assigned.

e. Actions, information, or material revealing spare parts availability for equipment or systems.

f. Actions, information, or material indicating equipment or system reliability (e.g., visits of technical representatives or special repair teams).

g. Movement of aircraft, ships, and ground units in response to friendly sensor detections of hostile units.

h. Actions, information, or material revealing tactics, techniques, and procedures employed in different types of training exercises or during equipment or system operational tests and evaluations.

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

2. Indicators of General Command and Control Capabilities

a. Actions, information, or material providing insight into the volume of orders and reports needed to accomplish tasks.

b. Actions, information, or material showing unit subordination for deployment, mission, or task.

c. Association of particular commanders with patterns of behavior under stress or in varying tactical situations.

d. Information revealing problems of coordination between the commander's staff elements.

e. In exercises or operations, indications of the period between the occurrence of a need to act or react and the action taking place, of consultations that occur with higher commands, and of the types of actions initiated.

f. Unusual actions with no apparent direction reflected in communications.

3. General Indicators from Communications Usage

a. Alert and maintenance personnel using handheld radios or testing aircraft or vehicle radios.

b. Establishing new communications nets. These might reveal entities that have intrinsic significance for the operation or activity being planned or executed. Without conditioning to desensitize adversaries, the sudden appearance of new communications nets could prompt them to implement additional intelligence collection to discern friendly activity more accurately.

c. Suddenly increasing traffic volume or, conversely, instituting radio silence when close to the time of starting an operation, exercise, or test. Without conditioning, unusual surges or periods of silence may catch adversaries' attention and, at a minimum, prompt them to focus their intelligence collection efforts.

d. Using static call signs for particular units or functions and unchanged or infrequently changed radio frequencies. This usage also allows adversaries to monitor friendly activity more easily and add to their intelligence database for building an accurate appreciation of friendly activity.

e. Using stereotyped message characteristics that indicate particular types of activity that allow adversaries to monitor friendly activity more easily.

f. Requiring check-in and check-out with multiple control stations before, during, and after a mission (usually connected with air operations).

g. Using social media either personally or through the command, broadcasting movements, capabilities, locations, personnel, etc.

4. Sources of Possible Indicators for Equipment and System Capabilities

a. Unencrypted emissions during tests and exercises.

b. Public media, particularly technical journals.

c. Budget data that provide insight into the objectives and scope of a system research and development effort or the sustainability of a fielded system.

d. The equipment or system hardware itself.

e. Information on test and exercise schedules that allows adversaries to better plan the use of their intelligence collection assets.

f. Deployment of unique units, targets, and sensor systems to support tests associated with particular equipment or systems.

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

h. Information indicating special manning for tests or assembly of personnel with special skills from manufacturers known to be working on a particular contract.

i. Notices to mariners and airmen that might highlight test areas.

j. Stereotyped use of location, procedures, and sequences of actions when preparing for and executing test activity for specific types of equipment or systems.

k. Use of advertisements indicating that a company has a contract on a classified system or component of a system, possesses technology of military significance, or has applied particular principles of physics and specific technologies to sensors and the guidance components of weapons.

5. Indicators of Preparations for Operations or Activities

Many indicators may reveal data during the preparatory, as compared to the execution, phase of operations or activities. Many deal with logistic activity.

a. Provisioning of special supplies for participating elements.

b. Requisitioning unusual volumes of supply items to be filled by a particular date.

c. Increasing pre-positioning of ammunition, fuels, weapon stocks, and other classes of supply.

d. Embarking special units, installing special capabilities, and preparing unit equipment with special paint schemes.

e. Procuring large or unusual numbers of maps and charts for specific locations.

f. Making medical arrangements, mobilizing medical personnel, stockpiling pharmaceuticals and blood, and marshalling medical equipment.

g. Focusing friendly intelligence and reconnaissance assets against a particular area of interest.

h. Requisitioning or assigning an increased number of linguists of a particular language or group of languages from a particular region.

i. Initiating and maintaining unusual liaison with foreign nations for support.

j. Providing increased or tailored personnel training.

k. Holding rehearsals to test concepts of operation.

l. Increasing the number of trips and conferences for senior officials and staff members.

m. Sending notices to airmen and mariners and making airspace reservations.

n. Arranging for tugs and pilots.

o. Requiring personnel on leave or liberty to return to their duty locations.

p. Declaring unusual off-limits restrictions.

q. Preparing units for combat operations through equipment checks, as well as operational standdowns in order to achieve a required readiness level for equipment and personnel.

r. Making billeting and transportation arrangements for particular personnel or units.

s. Taking large-scale action to change mail addresses or arrange for mail forwarding.

t. Posting such things as supply delivery, personnel arrival, transportation, or ordnance loading schedules in a routine manner where personnel without a need to know will have access.

u. Storing boxes or equipment labeled with the name of an operation or activity or with a clear unit designation outside a controlled area.

v. Employing uncleared personnel to handle materiel used only in particular types of operations or activities.

w. Providing unique or highly visible physical security arrangements for loading or guarding special munitions or equipment.

x. Requesting unusual or increased meteorological, oceanographic, or ice information for a specific area.

y. Setting up a wide-area network (WAN) over commercial lines.

6. Sources of Indicators During the Execution Phase

a. Unit and equipment departures from normal bases.

b. Adversary heat/infrared, radar, sonar, audio, or visual detections of friendly units.

c. Friendly unit identifications through COMSEC violation or physical observation of unit symbology.

d. Force composition and tracks or routes of advance that can be provided by emissions from units or equipment and systems that provide identifying data.

e. Stereotyped procedures; static and standard ways of composing, disposing, and controlling strike or defensive elements against particular threats; and predictable reactions to adversary actions.

f. Alert of civilians in operational areas.

g. Trash and garbage dumped by units or from ships at sea that might provide unit identifying data.

h. Transportation of spare parts or personnel to deploying or deployed units via commercial aircraft or ship.

i. Changes in oceanography high-frequency facsimile transmissions.

j. Changes in the activity over WAN.

7. Indicators of Post-Engagement Residual Capabilities

a. Repair and maintenance facilities schedules.

b. Urgent calls for maintenance personnel.

c. Movement of supporting resources.

d. Medical activity.

e. Unusual resupply and provisioning of an activity.

f. Assignment of new units from other areas.

g. Search and rescue activity.

h. Personnel orders.

i. Discussion of repair and maintenance requirements in unsecure areas.

j. Termination or modification of procedures for reporting unclassified meteorological, oceanographic, or ice information.

Intentionally Blank

APPENDIX B
FUNCTIONAL OUTLINES AND PROFILES

1. Intelligence Collection Operations

a. **General.** The completed intelligence profile reflects a picture of the intelligence collection effort. Intelligence collection is normally one of the first functional areas to present indicators of an impending operation or activity.

b. **Planned Event Sequence.** See the intelligence collection plan prepared by intelligence staff element.

c. **Actual Event Sequence.** Observe events in the joint intelligence operations center.

d. **Analysis.** Determine any OPSEC vulnerabilities. If vulnerabilities exist, determine whether they exist because of an error or because they are the result of normal procedures.

e. **Examples of Typical Indicators**

(1) Appearance of specialized intelligence collection equipment in a particular area.

(2) Increased traffic on intelligence communications nets.

(3) Increased manning levels and/or work hours in intelligence facilities.

(4) Increased research activities and personnel in libraries and electronic databases.

(5) Increased activity of friendly agent nets.

(6) Increased levels of activity by airborne intelligence systems.

(7) Alterations in the orbits of intelligence satellites.

(8) Interviews with nongovernmental subject matter experts conducted by intelligence personnel.

(9) Requests for maps and other topographic material.

(10) Appearance of OPSEC assessment team.

2. Logistics

a. **General.** The completed logistic profile presents a picture of logistic activities conducted in preparation for an impending operation. As in the administration function, the long lead time for some preparations gives early warning of forthcoming operations if events are compromised.

b. **Planned Event Sequence.** See logistic annex to OPLAN.

c. **Actual Event Sequence.** Observation, interviews.

d. **Analysis.** As conducted for the intelligence functional areas.

e. **Examples of Typical Indicators**

(1) Special equipment issue.

(2) Pre-positioning of equipment and supplies.

(3) Increased weapons and vehicle maintenance.

(4) Petroleum, oils, and lubricants stockpiling.

(5) Upgrading lines of communications.

(6) Ammunition stockpiling.

(7) Delivery of special munitions and uncommon munitions (discloses possible nature of operation).

(8) Arrival of new logistic units and personnel.

(9) Increased requisition of supplies.

(10) Increased traffic on logistic communications nets.

(11) Changes in normal delivery patterns.

(12) Appearance of OPSEC assessment team.

3. Communications

a. **General.** The completed communications profile reflects a picture of its own functional area, friendly communications also reflect all other functional areas. Communications surveillance and communications logs for all functional nets are important tools in evaluating this functional area, as well as other functions involved.

b. **Planned Event Sequence.** OPLAN, OPORD, signal operation instructions, or standing signal instruction.

c. **Actual Event Sequence.** Communications monitoring and communications logs.

d. **Analysis.** As conducted for the intelligence functional areas.

e. **Examples of Typical Indicators**

(1) Increased radio and telephone traffic.

(2) Increased communications checks.

(3) Appearance of new stations in net.

(4) New frequency and call-sign assignments.

(5) New codes and authenticators.

(6) Radio silence.

(7) Changing call-up patterns.

(8) Use of maintenance frequencies to test equipment.

(9) Communications command post exercises.

(10) Appearance of different cryptographic equipment and materials.

(11) Unclassified network activity.

(12) Appearance of OPSEC assessment team.

4. Operations

a. **General.** The completed profile of operational activities reflects events associated with units as they prepare for an operation.

b. **Planned Event Sequence.** OPLAN, OPORD, SOP.

c. **Actual Event Sequence.** Observations, reports, messages, interviews.

d. **Analysis.** As conducted for the intelligence functional areas.

e. **Examples of Typical Indicators**

(1) Rehearsals and drills.

(2) Special tactics refresher training.

(3) Appearance of special-purpose units (bridge companies, forward air controllers, pathfinders, mobile weather units).

(4) Pre-positioning of artillery and aviation units.

(5) Artillery registration in new objective area.

(6) Complete cessation of activity in area in which reconnaissance activity previously took place.

(7) Appearance of new attached units.

(8) Issuance of new equipment.

(9) Changes in major unit leadership.

(10) Repositioning of maneuver units.

(11) Appearance of OPSEC assessment team.

5. Administration and Support

a. **General.** The completed profile of administrative and support events shows activities taking place before the operation, thereby giving advance warning.

b. **Planned Event Sequence.** Derive from unit SOPs and administrative orders.

c. **Actual Event Schedule.** Observations and interviews.

d. **Analysis.** As conducted for the intelligence functional areas.

e. **Examples of Typical Indicators**

(1) Release of groups of personnel or complete units for personal affairs.

(2) Runs on exchanges for personal articles, cleaning, and other items.

(3) Changes to wake-up and dining schedules.

(4) Changes to mailing addresses.

(5) New unit designators on mail.

(6) Emergency personnel requisitions and fills for critical skills.

(7) Medical supply stockpiling.

(8) Emergency recall of personnel on pass and leave.

(9) Appearance of OPSEC assessment team.

(10) Increased activity at administrative/support offices, including processing of wills by legal department.

APPENDIX C
SAMPLE OPERATIONS SECURITY PLAN

OPLAN/OPORD: Tab C (Operations Security) to Appendix 3 (Information Operations) to Annex C (Operations)

Reference: JP 3-13.3, *Operations Security.*

1. ( ) **Situation.** Refer to other annexes and paragraphs in the basic plan as much as possible to avoid duplication. When publishing the OPSEC annex separately from the basic order, it is necessary to copy the information here in detail. This allows the OPSEC annex to be a useful, stand-alone document.

a. ( ) **Enemy Forces**

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

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

b. ( ) **Friendly Forces**

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

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

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

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

3. ( ) **Execution**

a. ( ) **Concept of Operations.** Describe the general concept to implement OPSEC countermeasures. Give it by phase and major activity (maneuver, logistics, communications, and so forth), if appropriate. Address OPSEC support to other elements of the IO plan, if applicable.

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

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

d. **Feedback.** Describe the concept for monitoring the effectiveness of OPSEC countermeasures during execution. Identify specific intelligence requirements for feedback.

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

f. **After-Action Reports.** Identify any requirements for after-action reporting.

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

5. ( ) **Command and Control**

a. ( ) **Command relationships**

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

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

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

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

APPENDIX D
REFERENCES

The development of JP 3-13.3 is based on the following primary references:

1. Department of Defense Publications

a. DOD Directive 5205.02, *DOD Operations Security (OPSEC) Program.*

b. DOD 5205.02-M, *DOD Operations Security (OPSEC) Program Manual.*

2. Chairman of the Joint Chiefs of Staff Publications

a. CJCSI 3210.03C, *Joint Electronic Warfare Policy*.

b. CJCSI 3211.01E, *Joint Policy for Military Deception*.

c. CJCSI 3213.01C, *Joint Operations Security*.

d. CJCSI 3320.01B, *Electromagnetic Spectrum Use in Joint Military Operations.*

e. CJCSI 5120.02B, *Joint Doctrine Development System*.

f. Chairman of the Joint Chiefs of Staff Manual (CJCSM) 3122.01A, *Joint Operation Planning and Execution System (JOPES), Volume I: (Planning Policies and Procedures).*

g. CJCSM 3122.03B, *Joint Operation Planning and Execution System (JOPES), Volume II: (Planning Formats).*

h. CJCSM 5714.01C, *Policy for Release of Joint Information*.

i. JP 1, *Doctrine for the Armed Forces of the United States*.

j. JP 1-02, *Department of Defense Dictionary of Military and Associated Terms*.

k. JP 2-0, *Joint Intelligence.*

l. JP 3-0, *Joint Operations*.

m. JP 3-13, *Information Operations.*

n. JP 3-13.1, *Electronic Warfare.*

o. JP 3-13.2, *Military Information Support Operations.*

p. JP 3-13.4, *Military Deception*.

q. JP 3-61, *Public Affairs*.

r. JP 5-0, *Joint Operation Planning*.

APPENDIX E
ADMINISTRATIVE INSTRUCTIONS

1. User Comments

Users in the field are highly encouraged to submit comments on this publication to: Joint Staff J-7, Deputy Director, Joint and Coalition Warfighting, Joint and Coalition Warfighting Center, ATTN: Joint Doctrine Support Division, 116 Lake View Parkway, Suffolk, VA 23435-2697. These comments should address content (accuracy, usefulness, consistency, and organization), writing, and appearance.

2. Authorship

The lead agent and the Joint Staff doctrine sponsor for this publication is the Director for Operations (J-3/J-39).

3. Supersession

This publication supersedes JP 3-13.3, *Operations Security*, 29 June 2006.

4. Change Recommendations

a. Recommendations for urgent changes to this publication should be submitted:

TO: JOINT STAFF WASHINGTON DC//J3//DDGO
INFO: JOINT STAFF WASHINGTON DC//J7-JEDD//

b. Routine changes should be submitted electronically to the Deputy Director, Joint and Coalition Warfighting, Joint and Coalition Warfighting Center, Joint Doctrine Support Division and info the lead agent and the Director for Joint Force Development, J-7/JEDD.

c. When a Joint Staff directorate submits a proposal to the CJCS that would change source document information reflected in this publication, that directorate will include a proposed change to this publication as an enclosure to its proposal. The Services and other organizations are requested to notify the Joint Staff J-7 when changes to source documents reflected in this publication are initiated.

5. Distribution of Publications

Local reproduction is authorized and access to unclassified publications is unrestricted. However, access to and reproduction authorization for classified JPs must be in accordance with DOD 5200.1-R, *Information Security Program*.

6. Distribution of Electronic Publications

a. Joint Staff J-7 will not print copies of JPs for distribution. Electronic versions are available on JDEIS at https://jdeis.js.mil (NIPRNET) and http://jdeis.js.smil.mil (SIPRNET), and on the JEL at http://www.dtic.mil/doctrine (NIPRNET).

b. Only approved JPs and joint test publications are releasable outside the combatant commands, Services, and Joint Staff. Release of any classified JP to foreign governments or foreign nationals must be requested through the local embassy (Defense Attaché Office) to DIA, Defense Foreign Liaison/IE-3, 200 MacDill Blvd., Joint Base Anacostia-Bolling, Washington, DC 20340-5100.

c. JEL CD-ROM. Upon request of a joint doctrine development community member, the Joint Staff J-7 will produce and deliver one CD-ROM with current JPs. This JEL CD-ROM will be updated not less than semi-annually and when received can be locally reproduced for use within the combatant commands and Services.

GLOSSARY

PART I—ABBREVIATIONS AND ACRONYMS

APEX	Adaptive Planning and Execution
C2	command and control
CCDR	combatant commander
CI	counterintelligence
CIL	critical information list
CJCS	Chairman of the Joint Chiefs of Staff
CJCSI	Chairman of the Joint Chiefs of Staff instruction
CJCSM	Chairman of the Joint Chiefs of Staff manual
CMOC	civil-military operations center
COA	course of action
COMSEC	communications security
CUI	controlled unclassified information
DIA	Defense Intelligence Agency
DIRNSA	Director, National Security Agency
DOD	Department of Defense
EEFI	essential element of friendly information
HUMINT	human intelligence
IA	information assurance
IGO	intergovernmental organization
IO	information operations
IOSS	Interagency Operations Security Support Staff
J-3	operations directorate of a joint staff
J-7	Joint Staff Directorate for Joint Force Development
JCMOTF	joint civil-military operations task force
JFC	joint force commander
JIACG	joint interagency coordination group
JIOWC/JOSE	joint information operations warfare center/joint operations security support element
JIPOE	joint intelligence preparation of the operational environment
JP	joint publication
JPG	joint planning group
LNO	liaison officer
MILDEC	military deception
MOE	measure of effectiveness

MOP	measure of performance
NGO	nongovernmental organization
NSA	National Security Agency
OEG	operations security executive group
OPLAN	operation plan
OPORD	operation order
OPSEC	operations security
PA	public affairs
PAO	public affairs officer
SIGINT	signals intelligence
SOP	standard operating procedure
WAN	wide-area network

PART II—TERMS AND DEFINITIONS

authenticator. A symbol or group of symbols, or a series of bits, selected or derived in a prearranged manner and usually inserted at a predetermined point within a message or transmission for the purpose of attesting to the validity of the message or transmission. (Approved for incorporation into JP 1-02 with JP 3-13.3 as the source JP.)

communications security equipment. None. (Approved for removal from JP 1-02.)

non-US forces. None. (Approved for removal from JP 1-02.)

operations security. A process of identifying critical information and subsequently analyzing friendly actions attendant to military operations and other activities. Also called **OPSEC.** (Approved for incorporation into JP 1-02.)

operations security assessment. An evaluative process, usually exercise, or support function to determine the likelihood that critical information can be protected from the adversary's intelligence. (Approved for inclusion in JP 1-02.)

operations security indicators. Friendly detectable actions and open-source information that can be interpreted or pieced together by an adversary to derive critical information. (JP 1-02, SOURCE: JP 3-13.3)

operations security countermeasures. Methods and means to gain and maintain essential secrecy about critical information. (Approved for replacement of "operations security measures" in JP 1-02.)

operations security planning guidance. Guidance that defines the critical information requiring protection from the adversary and outlines provisional measures to ensure secrecy. (Approved for incorporation into JP 1-02.)

operations security survey. A collection effort by a team of subject matter experts to reproduce the intelligence image projected by a specific operation or function simulating hostile intelligence processes. (Approved for inclusion in JP 1-02.)

operations security vulnerability. A condition in which friendly actions provide operations security indicators that may be obtained and accurately evaluated by an adversary in time to provide a basis for effective adversary decision making. (Approved for incorporation into JP 1-02.)

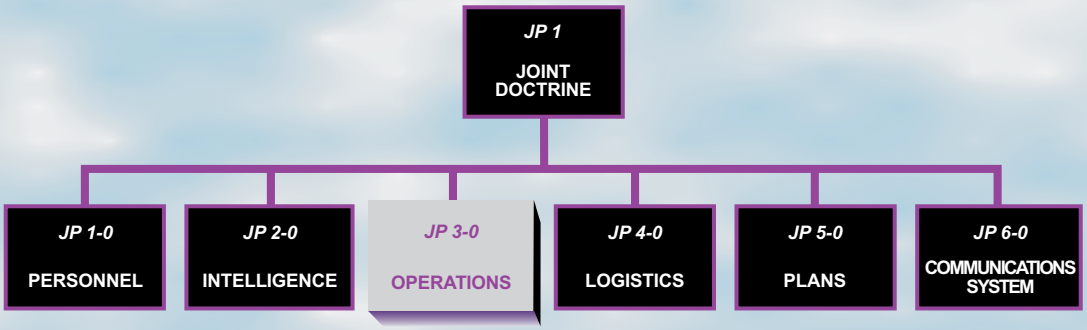
pathfinders. 1. Experienced aircraft crews who lead a formation to the drop zone, release point, or target. 2. Teams dropped or air landed at an objective to establish and operate navigational aids for the purpose of guiding aircraft to drop and landing zones. 3. A radar device used for navigating or homing to an objective when visibility precludes accurate visual navigation. 4. Teams air delivered into enemy territory for the purpose of determining the best approach and withdrawal lanes, landing zones, and sites for helicopterborne forces. (Approved for incorporation into JP 1-02 with JP 3-13.3 as the source JP.)

signal security. A generic term that includes both communications security and electronics security. (Approved for incorporation into JP 1-02 with JP 3-13.3 as the source JP.)

sonar. None. (Approved for removal from JP 1-02.)

sonobuoy. None. (Approved for removal from JP 1-02.)

JOINT DOCTRINE PUBLICATIONS HIERARCHY



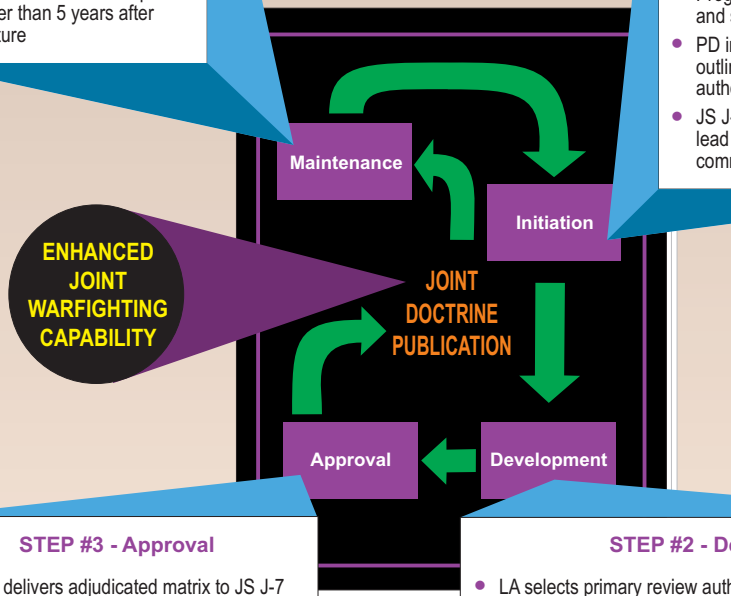
All joint publications are organized into a comprehensive hierarchy as shown in the chart above. **Joint Publication (JP) 3-13.3** is in the **Operations** series of joint doctrine publications. The diagram below illustrates an overview of the development process:

STEP #4 - Maintenance

- JP published and continuously assessed by users
- Formal assessment begins 24-27 months following publication
- Revision begins 3.5 years after publication
- Each JP revision is completed no later than 5 years after signature

STEP #1 - Initiation

- Joint doctrine development community (JDDC) submission to fill extant operational void
- Joint Staff (JS) J-7 conducts front-end analysis
- Joint Doctrine Planning Conference validation
- Program directive (PD) development and staffing/joint working group
- PD includes scope, references, outline, milestones, and draft authorship
- JS J-7 approves and releases PD to lead agent (LA) (Service, combatant command, JS directorate)



STEP #3 - Approval

- JSDS delivers adjudicated matrix to JS J-7
- JS J-7 prepares publication for signature
- JSDS prepares JS staffing package
- JSDS staffs the publication via JSAP for signature

STEP #2 - Development

- LA selects primary review authority (PRA) to develop the first draft (FD)
- PRA develops FD for staffing with JDDC
- FD comment matrix adjudication
- JS J-7 produces the final coordination (FC) draft, staffs to JDDC and JS via Joint Staff Action Processing (JSAP) system
- Joint Staff doctrine sponsor (JSDS) adjudicates FC comment matrix
- FC joint working group

JOINT
CHIEFS OF STAFF