Joint Publication 3-13.3

Operations Security

29 June 2006

PREFACE

1. Scope

This publication provides doctrine for planning, preparation, execution, and assessment of operations security in joint operations.

2. Purpose

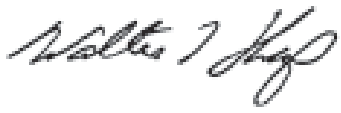
This publication has been prepared under the direction of the Chairman of the Joint Chiefs of Staff. It sets forth joint doctrine to govern the activities and performance of the Armed Forces of the United States in operations and provides the doctrinal basis for interagency coordination and for US military 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 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 commanders of 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:



WALTER L. SHARP
Lieutenant General, USA
Director, Joint Staff

Intentionally Blank

SUMMARY OF CHANGES
REVISION OF JOINT PUBLICATION 3-13.3 (FORMERLY 3-54) DATED 24 JANUARY 1997

- **Changes publication number from 3-54 to 3-13.3**
- **Adds a discussion of the operational context of operations security (OPSEC)**
- **Covers the purpose of OPSEC**
- **Discusses OPSEC as a core capability of information operations (IO)**
- **Lists OPSEC responsibilities for specific offices, commands, organizations, and staffs**
- **Covers the role of the IO cell in OPSEC planning**
- **Revises the discussion of OPSEC planning and joint operation planning processes**
- **Revises the definitions of the terms "operations security" and "operations security measures"**

Intentionally Blank

TABLE OF CONTENTS

FIGURE

EXECUTIVE SUMMARY
COMMANDER'S OVERVIEW

- **Provides an Overview of Operations Security (OPSEC)**
- **Delineates the Roles and Responsibilities of Key Individuals With Respect to OPSEC**
- **Explains the OPSEC Process**
- **Outlines Key Factors in OPSEC Planning**

Operations Security Overview

Operations security's (OPSEC's) most important characteristic is that it is a process.

Operations security (OPSEC) is a process that identifies critical information to determine if friendly actions can be observed by adversary intelligence systems, determines if information obtained by adversaries could be interpreted to be useful to them, and then executes selected measures that eliminate or reduce adversary exploitation of friendly critical information.

OPSEC is a methodology that denies critical information to an adversary. Unlike security programs that seek to protect classified information, OPSEC measures identify, control, and protect generally unclassified evidence that is associated with sensitive operations and activities.

Responsibilities

Key roles and responsibilities.

Chairman of the Joint Chiefs of Staff (CJCS) advises and coordinates with the Secretary of Defense concerning OPSEC support to the combatant commands and provides joint OPSEC policy and doctrine.

Director for Operations (J-3), Joint Staff executes primary Joint Staff responsibility for OPSEC and designates OPSEC staff positions for the Joint Staff. Another key J-3 responsibility is to establish the OPSEC executive groups (OEGs), as necessary, comprised 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.

Service Chiefs provide Service OPSEC policy, doctrine, and planning procedures consistent with OPSEC policy, doctrine, and guidance. In addition, they provide OPSEC awareness training assistance for general populations, leadership, and OPSEC program managers; organize teams to conduct vulnerability assessments of subordinate commands; and designate an OPSEC program officer in the operations element of the Service headquarters as well as representatives to Joint Staff OEGs, when required.

Joint force commanders (JFCs) provide OPSEC guidance and identify command-critical information to all supporting commands, subordinate commands, other agencies, and appropriate public affairs offices. JFCs also coordinate OPSEC measures and their execution with other commands and agencies of those activities.

OPSEC Program Officers advise the commander on all OPSEC-related matters and manage the organization's OPSEC program. In addition, they provide OPSEC input to information operations (IO) planning and develop, maintain, and monitor the execution of the organization's OPSEC program.

Director, Defense Intelligence Agency conducts analysis of the foreign intelligence collection threat for use in OPSEC measures and provides results to CJCS, Service Chiefs, combatant commanders, and heads of Department of Defense (DOD) agencies.

Director, National Security Agency (NSA), Interagency OPSEC Support Staff (IOSS) assists DOD components in establishing OPSEC programs, as requested. NSA IOSS also collaborates with the heads of the DOD components by providing technical OPSEC assessment support to DOD components; recommendations relating to doctrine, methods, and procedures to minimize vulnerabilities; communications and computer security support for OPSEC assessments; signals intelligence support for OPSEC threat development; and red and blue team OPSEC assessments.

OPSEC is an information operations core capability.

OPSEC denies the adversary the information needed to correctly assess friendly capabilities and intentions. In particular, OPSEC complements military deception by denying an adversary information required to both assess a real plan and to disprove a deception plan. OPSEC is essential when conducting IO to ensure

friendly capabilities that might be easily countered are not compromised.

The Operations Security Process

The OPSEC process is applicable across the range of military operations.

The OPSEC 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.

There are five distinct actions of the OPSEC process.

The OPSEC process consists of five distinct actions.

Identification of Critical Information. The identification of critical information (information that is vitally needed by an adversary) is important in that it focuses the remainder of the OPSEC process on protecting vital information, rather than attempting to protect all classified or sensitive unclassified information.

Analysis of Threats. This action involves the research and analysis of intelligence, counterintelligence, and open source information to identify who the likely adversaries are in the planned operation.

Analysis of Vulnerabilities. This action involves examining each aspect of the planned operation to identify OPSEC indicators that could reveal critical information and then comparing those indicators with the adversary's intelligence collection capabilities identified in the previous action.

Assessment of Risk. First, planners analyze the vulnerabilities identified in the previous action and identify possible OPSEC measures for each vulnerability. Second, specific OPSEC measures are selected for execution based upon a risk assessment done by the commander and staff.

Application of Appropriate OPSEC Measures. The command implements the OPSEC measures selected in the assessment of risk action or, in the case of planned future operations and activities, includes the measures in specific OPSEC plans.

Additionally, an **OPSEC assessment** is an intensive application of the OPSEC process to an existing operation or activity by a multidisciplined team of experts. Assessments are essential for

identifying requirements for additional OPSEC measures and for making necessary changes in existing OPSEC measures.

Operations Security Planning Considerations

OPSEC planning and execution occur as part of the organization's information operations effort.

The following factors must be considered when conducting OPSEC planning:

1. The commander plays the critical role.

2. OPSEC is an operations function, not a security function.

3. JFCs should establish a fully functional IO cell.

4. Planning must focus on identifying and protecting critical information.

5. The ultimate goal of OPSEC is increased mission effectiveness.

6. OPSEC is one of the factors considered during the development and selection of friendly courses of action.

7. OPSEC planning is a continuous process.

8. The public affairs officer participates in OPSEC planning to provide assessments on the possible negative effects of media coverage and all other public release of information by members of the command and for the coordination of OPSEC measures and public affairs ground rules to minimize those effects.

9. OPSEC considers the integration, coordination, deconfliction, and synchronization of all multinational information activities within the JFC's operational area.

10. The termination of OPSEC measures must be addressed in the OPSEC plan to prevent future adversaries from developing countermeasures to successful OPSEC measures.

OPSEC and multinational operations.

OPSEC measures that apply to joint operations are appropriate also for multinational situations conducted within the structure of an alliance or coalition. In these situations the collection, production, and dissemination of intelligence can be a major challenge. Since alliance or coalition 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. The National Disclosure Policy provides initial guidance.

CONCLUSION

This publication provides joint doctrine to guide the Armed Forces in the conduct of OPSEC operations. It describes the OPSEC framework, discusses key roles and responsibilities, explains the OPSEC process, and outlines key considerations for OPSEC planning.

Intentionally Blank

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) 3213.01B, *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 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 presents a pattern of behavior. Furthermore, certain unique, particular, or special types of information might also be associated with an activity or operation. Although much of this information may be unclassified, when correlated with other bits of unclassified information, they may become classified or revealing of a sensitive operation.

b. An **indicator** is a type, or class, of information that is significantly associated with or characteristic of an activity. Selected indicators can be developed into an analytical **model** or profile of how a force gets ready and how it operates. An **indication** is an observed specific occurrence or instance of an indicator. As described, an indicator is also known as an essential element of friendly information (EEFI) or a bit of data the adversary or enemy is trying to collect against friendly forces. Friendly forces try to collect essential elements of information on enemy forces.

c. Intelligence personnel analyze and interpret collected information to identify indications for comparison with the model. As analysts apply more information to the model, the likelihood increases that the observed force is actually following the model. Thus, current and future capabilities and courses of action can be revealed and compromised. **Critical information** consists of the significant information and indications that can be used by the adversary commander to gain real advantage, and perhaps decisively assure success or preclude failure.

d. To prevent or reduce successful adversary collection and exploitation of US critical information, the commander must create a prudently formulated, practical, timely, and effective operations security program.

3. Purpose of Operations Security

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

b. **OPSEC is a process** of identifying critical information and subsequently analyzing 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. The commander must know the model or profile of his or her organization.

(3) Select and execute measures that eliminate or reduce to the visibility of joint forces to observation and exploitation. The commander must whenever feasible:

(a) Avoid patterns of behavior and thus preclude the possibility of adversary intelligence constructing an accurate model.

(b) Avoid the model.

(c) Prevent the display or collection of critical information — especially during preparation for and conduct of actual combat operations.

c. A special challenge to OPSEC is to get it right — to match belief and action to reality. In the OPSEC process, there is information that the adversary force thinks it requires and tasks its intelligence agencies to collect and analyze. There is also information that the US force thinks it must protect because it may provide indications of current and future operations. The US force believes that it must keep the adversary force from observing and understanding these actions and assets. In contrast, there is critical information that **might actually assure success** (or prevent failure). The adversary force may not know it needs this information. The US force may not realize it must conceal it. Successful OPSEC demands the US force conceal that critical information which actually would offer success to the adversary commander.

4. 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 that can be applied to every operation. **It is a method 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, OPSEC is concerned with **identifying**, **controlling**, and **protecting unclassified evidence** that is associated with

military operations and activities. **OPSEC and security programs must be closely coordinated** to ensure appropriate aspects of military operations are protected.

c. Some level of risk must be assumed when choosing whether or not to execute OPSEC measures. OPSEC measures, in most cases, involve the expenditure of resources. In choosing to execute particular OPSEC measures, commanders must 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 risks. The OPSEC process demands that decision makers directly address what is acceptable risk and how much the decision makers are willing to assume. Current safety and security rules should also be considered, and may limit a commander's assumption of risk, without first obtaining appropriate waivers.

d. **Operations Security as a Core Capability of Information Operations (IO).** OPSEC denies the adversary the information needed to correctly assess friendly capabilities and intentions. It is also a tool of IO itself, hampering the adversary's use of his 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. For those 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 essential elements of friendly information and taking 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 information assurance (IA), computer network defense, and personnel programs that screen personnel and limit authorized access.

5. Responsibilities

Listed below are the key OPSEC responsibilities for specific offices, commands, or organizations, and staffs.

a. **Chairman of the Joint Chiefs of Staff (CJCS)**

(1) Advises and coordinates with the Secretary of Defense concerning OPSEC support to the combatant commands.

(2) Provides joint OPSEC policy and doctrine.

(3) Provides procedures for joint OPSEC support within the Joint Operation Planning and Execution System.

(4) Ensures that appropriate OPSEC measures are implemented during CJCS exercises.

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

(1) Executes primary Joint Staff responsibility for OPSEC.

(2) Designates OPSEC staff positions for the Joint Staff.

(3) Maintains a joint OPSEC lessons-learned database as a subset of the Joint Lessons Learned Program (JLLP). The JLLP database is maintained by the United States Joint Forces Command Joint Center for Operational Analysis and Lessons Learned, to support OPSEC planning and training by the Joint Staff, Services, combatant commands, and Department of Defense (DOD) agencies.

(4) Establishes and maintains an OPSEC orientation program for Joint Staff general population.

(5) Assists joint agencies and commands in arranging national interagency participation in OPSEC assessments.

(6) Coordinates with the Director for Operational Plans and Joint Force Development (J-7), Joint Staff, to ensure that OPSEC is adequately addressed and evaluated in operation plans (OPLANs), operation plans in concept format (CONPLANs), and operation orders (OPORDs).

(7) Assigns an OPSEC liaison officer during periods of crisis and during CJCS exercises to assist all Joint Staff elements in integrating OPSEC into crisis management planning efforts. The OPSEC liaison officer also serves as a point of contact to coordinate OPSEC issues with the combatant commands, DOD agencies, and Services.

(8) Establishes the OPSEC executive groups (OEGs), as necessary, comprised 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.

(9) Coordinates with the National Security Agency (NSA), Interagency OPSEC Support Staff (IOSS), the Defense Threat Reduction Agency, and United States Strategic Command's Joint Information Operations Center (JIOC)/Joint OPSEC Support Staff for OPSEC support.

c. **Military Departments/Service Chiefs**

(1) Provide Service OPSEC policy, doctrine, and planning procedures consistent with OPSEC policy, doctrine, and guidance.

(2) Provide OPSEC awareness training assistance for general populations, leadership, and OPSEC program managers.

(3) Designate an OPSEC program officer in the operations element of the Service headquarters.

(4) Designate representatives to Joint Staff OEGs, when required.

(5) Provide OPSEC lessons learned to the J-3 and J-7, Joint Staff, for inclusion in the OPSEC lessons-learned database.

(6) Provide to J-3, Joint Staff, copies of all current Service OPSEC program directives and/or policy implementation documents.

(7) Organize teams to conduct vulnerability assessments of subordinate commands.

d. **Joint Force Commanders**

(1) Commander, US Strategic Command will support other combatant commanders (CCDRs) for the planning and integration of joint OPSEC.

(2) Provide OPSEC guidance to subordinate commands and support their responsibilities for integrating OPSEC into all command operations, exercises, and other joint activities.

(3) Provide OPSEC guidance and identify command-critical information to all supporting commands, subordinate commands, other agencies, and appropriate public affairs (PA) offices.

(4) Coordinate OPSEC measures and their execution with other commands and agencies of those activities such as strategic command and control (C2) and counterdrug operations that cross command boundaries.

(5) Plan for and execute OPSEC measures in support of assigned missions across the range of military operations.

(6) Conduct OPSEC assessments in support of command operations.

(7) Designate an OPSEC program officer in the J-3 element of the command headquarters.

(8) Conduct annual OPSEC program reviews. Identify areas requiring additional CJCS guidance, assistance, or clarification to the combatant command.

(9) Conduct OPSEC lessons learned through the combatant command J-3 and update EEFIs as required.

(10) Provide to the combatant command copies of all current command OPSEC program directives and/or policy implementation documents.

(11) Provide OPSEC awareness training to assigned organizations.

e. **OPSEC Program Officer**

(1) Develops, presents, and provides materials for command OPSEC awareness and training.

(2) Manages the organization's OPSEC program.

(3) Advises the commander on all OPSEC-related matters, to include developing and recommending OPSEC policy, guidance, and instructions.

(4) Provides OPSEC input to IO planning.

(5) Develops, maintains, and monitors the execution of the OPSEC program.

(6) Coordinates and/or conducts OPSEC assessments.

(7) Coordinates intelligence support.

(8) Coordinates counterintelligence and counterespionage support.

(9) Coordinates force protection, antiterrorism, and security support.

(10) Coordinates for PA support.

(11) Compiles subordinate organization critical information for consolidation into command critical information lists.

(12) Coordinates for civil-military operations, civil affairs and host-nation support.

(13) Incorporates exercise scenarios and events into exercises.

f. **Director, Defense Intelligence Agency (DIA)**

(1) Establishes and maintains an OPSEC training program for DIA civilian and military personnel.

(2) Designates an agency OPSEC program officer.

(3) Designates representatives to Joint Staff OEGs, as required.

(4) Identifies, reviews, and validates DIA and other DOD counterintelligence threat assessment documents for Joint Staff use.

(5) Conducts analysis of the foreign intelligence collection threat for use in OPSEC measures. Provides results to the Chairman of the Joint Chiefs of Staff, Service Chiefs, CCDRs, and heads of DOD agencies.

g. **Director, National Security Agency, Interagency OPSEC Support Staff**

(1) Assists DOD components in establishing OPSEC programs, as requested.

(2) Provides interagency OPSEC training courses.

(3) Designates representative to Joint Staff OEGs, as required.

(4) Collaborates with the heads of the DOD components by providing:

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

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

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

(d) Signals intelligence (SIGINT) support for OPSEC threat development.

(e) Red and blue team OPSEC assessments.

h. **Other DOD Agencies and Joint Activities**

(1) Designate an agency OPSEC program officer.

(2) Coordinate OPSEC programs and activities with commands and other agencies, as required.

(3) Provide representatives to Joint Staff OEGs, as required.

Intentionally Blank

CHAPTER II
THE OPERATIONS SECURITY PROCESS

"He passes through life most securely who has least reason to reproach himself with complaisance toward his enemies."

Thucydides,
***History of the Peloponnesian Wars*, 404 BC**

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 measures address all significant aspects of the particular situation and are balanced against operational requirements. OPSEC is a continuous process. **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 measures**.** 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.** 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. The Operations Security Process

The five OPSEC process (Figure II-1) actions are:

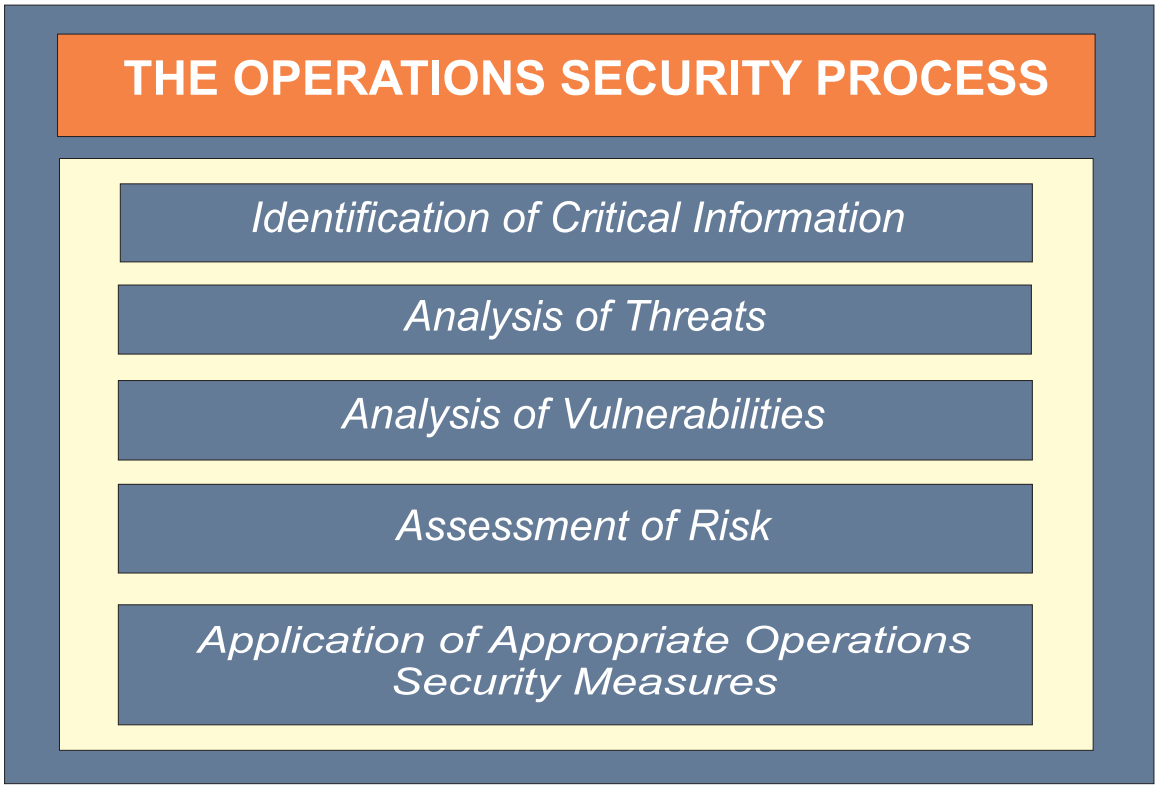


Figure II-1. The Operations Security Process

a. **Identification of Critical Information**

(1) The **identification of critical information** is important in that **it focuses the remainder of the OPSEC process on protecting vital information** rather than attempting to protect all classified or sensitive unclassified information.

(2) **Critical information is listed in the OPSEC portion of an OPLAN or OPORD.** Generic critical information lists can be developed beforehand to assist in identifying the specific critical information. Some general categories of critical information are provided in Appendix A, "Examples of Operations Security Critical Information."

b. **Analysis of Threats**

(1) This action involves the research and analysis of **intelligence**, **counterintelligence**, and **open source information** to identify who the likely adversaries are in the planned operation. Feedback on IO can provide information on adversarial personalities that assist in developing a threat analysis.

(2) **The operations planners**, working with the intelligence and counterintelligence staffs and assisted by the OPSEC program officer, **seek answers to the following critical information questions:**

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

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

(c) What is the adversary's course of action (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.)

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

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

c. **Analysis of Vulnerabilities**

(1) 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 that could reveal critical information and then comparing those indicators with the adversary's intelligence collection capabilities identified in the previous action. A vulnerability exists when the adversary is capable of collecting an OPSEC indicator, correctly analyzing it, and then taking timely action. The adversary can then exploit that vulnerability to obtain an advantage.

> *"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**

(2) Continuing to work with the intelligence and counterintelligence staffs, the operations planners seek answers to the following critical information questions:

(a) 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?

(b) What indicators can the adversary actually collect?

(c) 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?)

(3) See Appendix B, "Operations Security Indicators," for a detailed discussion of OPSEC indicators.

All personnel must understand the adversary's capability to collect information and take OPSEC measures to deny the use of that capability.

d. **Assessment of Risk**

(1) This action has two components. First, **planners analyze the vulnerabilities** identified in the previous action and **identify possible OPSEC measures** for each vulnerability. Second, **specific OPSEC measures are selected for execution** based upon a risk assessment done by the commander and staff.

(2) OPSEC measures reduce the probability of the adversary either collecting the indicators or being able to correctly analyze their meaning.

(a) **OPSEC measures can be used to:** prevent the adversary from detecting an indicator; provide an alternative analysis of an indicator (prevent the adversary from correctly interpreting the indicator); and/or attack the adversary's collection system.

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

(c) **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 measures are those that combine the highest possible protection with the least adverse effect on operational effectiveness. Appendix C, "Operations Security Measures," provides examples of OPSEC measures.

(3) **Risk assessment** requires comparing the estimated cost associated with implementing each possible OPSEC measure to the potential harmful effects on mission accomplishment resulting from an adversary's exploitation of a particular vulnerability.

(a) **OPSEC measures 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 measure entails risks, this step requires the commander's decision (or approval). Critical intelligence operations and sources may be compromised if OPSEC measures are applied. Some operations and collection methods/sources may be too important to be compromised if the adversary detects friendly OPSEC measures.

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

1. What risk to effectiveness is likely to occur if a particular OPSEC measure is implemented?

2. What risk to mission success is likely to occur if an OPSEC measure is not implemented?

3. What risk to mission success is likely if an OPSEC measure fails to be effective?

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

(4) **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 measures. Conversely, MILDEC and psychological operations plans may require that OPSEC measures not be applied to certain indicators in order to project a specific message to the adversary.

e. **Application of Appropriate OPSEC Measures**

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

(2) A general OPSEC measure strategy should be to:

(a) Minimize predictability from previous operations.

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

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

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

(3) During the execution of OPSEC measures, **the adversary's reaction to the measures is monitored to determine their effectiveness and to provide feedback**. 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 counterintelligence 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 measures.

3. Operations Security Assessment

An OPSEC assessment is an **intensive application of the OPSEC process** to an existing operation or activity by a multidisciplined team of experts. Assessments are essential for **identifying requirements** for additional OPSEC measures and for **making necessary changes** in existing OPSEC measures. An OPSEC assessment is a good tool to validate OPSEC programs and organizational practices to protect critical information in operations. NSA, IOSS, the JIOC, and the Services have or can coordinate red and blue teams designed to act as an adversary to verify OPSEC plans and procedures. In addition to seeking support from external commands,

the joint force commander (JFC) should attempt to utilize internal capabilities to conduct OPSEC assessments. Appendix D, "Procedures for Operations Security Assessments," describes the procedures for conducting OPSEC assessments.

Intentionally Blank

CHAPTER III
OPERATIONS SECURITY PLANNING

"To keep your actions and your plans secret always has been a very good thing . . . Marcus Crassus said to one who asked him when he was going to move the army: 'Do you believe that you will be the only one not to hear the trumpet?"

Niccolo Machiavelli, *The Art of War*, 1521

1. General

a. Despite extraordinary changes in the world geopolitical environment in recent years, many nations and organizations are actively engaged in conducting intelligence operations against the US and its armed forces. Open-source material (including the media and the Internet) and observations of US activities and operations are major sources of information for the adversary. This is especially true of terrorist organizations.

b. In order to prevent adversaries (or potential adversaries) from gaining critical information concerning friendly operations, joint forces must plan and execute OPSEC measures. To be effective, OPSEC measures 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.

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

c. OPSEC planning and execution occur as part of the command's or organization's IO effort. The commander's objectives are the basis for OPSEC planning. OPSEC measures can be considered along, or in conjunction with other IO capabilities.

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 must be provided as part of the commander's IO planning guidance to ensure that OPSEC is considered during the development of friendly COAs.

b. **OPSEC is an operations function, not a security function.** OPSEC planning is performed by the J-3 operations planners. The J-3 planners are assisted by the organization's OPSEC program officer 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. **JFCs should establish a fully functional 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. The OPSEC program officer plays a vital role in the IO cell. The OPSEC program officer coordinates combatant command or subordinate joint force OPSEC activities and coordinates with the communications systems directorate and J-3 planners for NSA's joint communications security (COMSEC) monitoring activity liaison.

d. **Planning must focus on identifying and protecting critical information.** Denying all information about a friendly operation or activity is seldom cost effective or realistic.

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 one of the factors 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 measures. 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 measures is evaluated based on measures of effectiveness and the OPSEC plan is modified accordingly. Friendly intelligence and counterintelligence organizations, COMSEC monitoring, and OPSEC assessments are the primary sources for feedback information and are continuous throughout the OPSEC planning process.

h. **The public affairs officer (PAO) participates in OPSEC planning** to provide assessments on the possible negative effects of media coverage and all other public release of information by members of the command and for the coordination of OPSEC measures and PA ground rules to minimize those effects. The PAO ensures that the media pool, media clearances, media releases, and authorization of video transmissions are within the established OPSEC measures. The PAO also ensures 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 Joint Publication (JP) 3-61, Public Affairs*, for further details.*

i. **OPSEC considers the integration, coordination, deconfliction, and synchronization of all multinational information activities within the JFC's operational area.**

> *"O divine art of subtlety and secrecy! Through you we learn to be invisible, through you inaudible; and hence hold the enemy's fate in our hands."*
>
> **Sun Tzu, c. 500 BC, *The Art of War***

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

3. Operations Security Planning Coordination

a. **General.** OPSEC coordination is continuous across **all phases of an operation** and **the range of military operatons** 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, 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 .

4. Operations Security Planning and Joint Operation Planning Processes

a. **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 normal joint operation planning and is a part of the overall IO planning effort.

b. **Campaign Planning Process.** A campaign is a series of related military operations aimed at accomplishing strategic and operational objectives within a given time and space. They are joint in nature and serve as the focus for military activities across the range of military operatons.

(1) CCDRs translate national and theater goals and objectives into strategic and operational concepts through the development of theater campaign plans. The campaign plan embodies the CCDR's strategic vision of the arrangement of related operations necessary to attain theater strategic objectives. Campaign planning encompasses both the contingency and crisis action planning processes. If the scope of contemplated operations requires it, campaign planning begins with or during contingency planning and continues through crisis action planning, thus unifying both planning processes. The degree to which the amount of work accomplished in contingency planning may serve as the core for a campaign plan is directly dependent on the particular theater and objectives.

(2) Preparation of a campaign plan is appropriate when contemplated military operations exceed the scope of a single major operation. Campaign planning is appropriate to both contingency and crisis action planning. During peacetime contingency planning, CCDRs prepare joint OPLANs, including campaign plans, in direct response to taskings in the Joint Strategic Capabilities Plan.

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

c. **OPSEC and the Contingency 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 appraised of all OPSEC contingency planning activities that may require synchronization, coordination, or deconfliction.

d. **OPSEC and the Crisis Action Planning Process.** In contrast to contingency planning, crisis action planning normally takes place in a compressed time period. In crisis action planning, coordination of the OPSEC plan is even more crucial than in contingency planning.

5. Operations Security and Multinational Operations

a. US military operations often are **conducted with the armed forces of other nations** in pursuit of common objectives.

b. Multinational operations, both those that include combat and those that do not, are conducted within the structure of an alliance or coalition.

(1) **An alliance** is a result of **formal agreements** between two or more nations for **broad, long-term objectives**. These alliance operations are combined operations, though in common usage combined often is used inappropriately as a synonym for all multinational operations.

(2) **A coalition** is an **ad hoc arrangement** between two or more nations for **common action**; for instance, the coalition that defeated Iraqi aggression against Kuwait in the Gulf War, 1990-1991.

c. Joint operations as part of an alliance or coalition **require close cooperation** among all forces and can serve to mass strengths, reduce vulnerabilities, and provide legitimacy. OPSEC measures that apply to joint operations are appropriate also for multinational situations.

d. Plans should be issued far enough in advance to allow sufficient time for member forces to conduct their own planning and rehearsals. Some alliance or coalition member 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 the capabilities of other member forces.

e. **Intelligence.** The collection, production, and dissemination of intelligence can be a major challenge. Alliance or coalition 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 the forces of other nations 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 negotiating authority. Applying the OPSEC process to intelligence can assist in determining what information can be shared with a coalition or alliance.

(2) **The National Disclosure Policy provides initial 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 that information that is mission essential, affects lower-level operations, facilitates combat identification, and is perishable.

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) pre-deployment 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 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

APPENDIX A
EXAMPLES OF OPERATIONS SECURITY CRITICAL INFORMATION

1. Introduction

This appendix provides general examples of OPSEC critical information. Several generic military activities with some of their associated critical information are listed. These are only a few of the many types of military activities and their associated critical information.

2. Diplomatic Negotiations

a. Military capabilities (pre-treaty and post-treaty).

b. Intelligence verification capabilities.

c. Minimum negotiating positions.

3. Politico-Military Crisis Management

a. Target selection.

b. Timing considerations.

c. Logistic capabilities and limitations.

d. Alert posture.

4. Military Intervention

a. Intentions.

b. Military capabilities.

c. Forces assigned and in reserve.

d. Targets.

e. Timing.

f. Logistic capabilities and constraints.

g. Limitations.

h. Third-nation support arrangements.

i. Location of communications system support nodes.

j. Frequency and callsigns.

k. Category/type (injury) of patient moved.

l. Movement by what means (aeromedical vs casualty evacuation vs medical evacuation).

5. Counterterrorism

a. Forces.

b. Targets.

c. Timing.

d. Staging locations.

e. Tactics.

f. Ingress and egress methods/routes.

g. Logistic capabilities and constraints.

h. Category/type (injury) of patient moved.

i. Movement by what means (aeromedical vs casualty evacuation vs medical evacuation).

6. Open Hostilities

a. Force composition and disposition.

b. Attrition and reinforcement.

c. Targets.

d. Timing.

e. Logistic constraints.

f. Location of critical communications system nodes.

7. Mobilization

a. Intent to mobilize before public announcement.

b. Impact on military industrial base.

c. Impact on civil economy.

d. Transportation capabilities and limitations.

e. Category/type (injury) of patient moved.

f. Movement by what means (aeromedical vs casualty evacuation vs medical evacuation).

8. Battlespace Awareness

a. Purpose of collection.

b. Targets of collection.

c. Timing.

d. Capabilities of collection assets.

e. Processing capabilities.

f. Unit requesting collection.

g. Unit conducting collection.

h. Communications capabilities.

9. Peacetime Weapons and Other Military Movements

a. Fact of movement.

b. Periodicity and trends of movements.

c. Origin and destination of equipment being moved.

d. Capabilities and limitations of equipment being moved.

e. Extent of inventory of equipment being moved.

10. Command Post, Computer-Aided, and Field Training Exercises

a. Participating units.

b. OPLANs, CONPLANs, or other contingencies that are being exercised.

c. Command relationships.

d. Communication systems connections and weaknesses.

e. Logistic capabilities and limitations.

11. Noncombatant Evacuation Operations (Permissive/Nonpermissive)

a. Targets.

b. Forces.

c. Logistic constraints.

d. Safe havens.

e. Routes.

f. Timing.

g. Category/type (injury) of patient moved.

h. Movement by what means (aeromedical vs casualty evacuation vs medical evacuation).

12. Counterdrug Operations

a. Identity of military forces.

b. Law enforcement agency (LEA) involvement.

c. Military support to LEAs.

d. Host-nation cooperation.

e. Capabilities.

f. Timing.

g. Tactics.

h. Logistic capabilities and constraints.

APPENDIX B
OPERATIONS SECURITY INDICATORS

1. Operations Security Indicators

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

2. Basic Operations Security Indicator Characteristics

An indicator's characteristics are those elements of an action or piece of information that are potentially useful to an adversary. There are five major characteristics.

a. **Signature**

(1) 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.

(2) 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.

(3) 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.

b. **Associations**

(1) 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 continuously 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.

(2) 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.

(3) 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.

c. **Profiles**

(1) 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.

(2) 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).

(3) 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.

(4) 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.

d. **Contrasts**

(1) 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 differences to established profiles. They also are simpler to use because they need only to be recognized, not understood.

(2) 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.

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

(a) Have bombers been deployed at fighter bases before? At this particular fighter base? At several fighter bases simultaneously?

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

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

(d) What actions occurred while the bombers were deployed at the fighter bases?

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

(f) Who will decide where, when, what, and how fighter bombers will deploy?

(4) 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.

e. **Exposure**

(1) 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.

(2) 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.

(3) 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 he can formulate questions and focus collection assets to provide answers if the indicator is observed again.

(4) 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.

3. Examples of 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.

a. **Indicators of General Military Force Capabilities**

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

(2) Friendly reactions to adversary exercises or actual hostile actions.

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

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

(5) Actions, information, or material revealing spare parts availability for equipment or systems.

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

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

(8) 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.

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

b. **Indicators of General C2 Capabilities**

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

(2) Actions, information, or material showing unit subordination for deployment, mission, or task.

(3) Association of particular commanders with patterns of behavior under stress or in varying tactical situations.

(4) Information revealing problems of coordination between the commander's staff elements.

(5) 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.

(6) Unusual actions with no apparent direction reflected in communications.

c. **General Indicators from Communications Usage**

(1) Alert and maintenance personnel using handheld radios or testing aircraft or vehicle radios.

(2) 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.

(3) 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.

(4) 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.

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

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

d. **Sources of Possible Indicators for Equipment and System Capabilities**

(1) Unencrypted emissions during tests and exercises.

(2) Public media, particularly technical journals.

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

(4) The equipment or system hardware itself.

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

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

(7) Unusual or visible security imposed on particular development efforts that highlight their significance.

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

(9) Notices to mariners and airmen that might highlight test areas.

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

(11) 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.

e. **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.

(1) Provisioning of special supplies for participating elements.

(2) Requisitioning unusual volumes of supply items to be filled by a particular date.

(3) Increasing pre-positioning of ammunition, fuels, weapon stocks, and other classes of supply.

(4) Embarking special units, installing special capabilities, and preparing unit equipment with special paint schemes.

(5) Procuring large or unusual numbers of maps and charts for specific locations.

(6) Making medical arrangements, mobilizing medical personnel, stockpiling pharmaceuticals and blood, and marshalling medical equipment.

(7) Focusing friendly intelligence and reconnaissance assets against a particular area of interest.

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

(9) Initiating and maintaining unusual liaison with foreign nations for support.

(10) Providing increased or tailored personnel training.

(11) Holding rehearsals to test concepts of operation.

(12) Increasing the number of trips and conferences for senior officials and staff members.

(13) Sending notices to airmen and mariners and making airspace reservations.

(14) Arranging for tugs and pilots.

(15) Requiring personnel on leave or liberty to return to their duty locations.

(16) Declaring unusual off-limits restrictions.

(17) 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.

(18) Making billeting and transportation arrangements for particular personnel or units.

(19) Taking large-scale action to change mail addresses or arrange for mail forwarding.

(20) 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.

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

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

(23) Providing unique or highly visible physical security arrangements for loading or guarding special munitions or equipment.

(24) Requesting unusual or increased meteorological, oceanographic, or ice information for a specific area.

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

f. **Sources of Indicators During the Execution Phase**

(1) Unit and equipment departures from normal bases.

(2) Adversary radar, sonar, or visual detections of friendly units.

(3) Friendly unit identifications through COMSEC violation or physical observation of unit symbology.

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

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

(6) Alert of civilians in operational areas.

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

(8) Transportation of spare parts or personnel to deploying or deployed units via commercial or aircraft or ship.

(9) Changes in oceanography high frequency facsimile transmissions.

(10) Changes in the activity over WAN.

g. **Indicators of Post Engagement Residual Capabilities**

(1) Repair and maintenance facilities schedules.

(2) Urgent calls for maintenance personnel.

(3) Movement of supporting resources.

(4) Medical activity.

(5) Unusual resupply and provisioning of an activity.

(6) Assignment of new units from other areas.

(7) Search and rescue activity.

(8) Personnel orders.

(9) Discussion of repair and maintenance requirements in unsecure areas.

(10) Termination or modification of procedures for reporting of unclassified meteorological, oceanographic, or ice information.

Intentionally Blank

APPENDIX C
OPERATIONS SECURITY MEASURES

1. Introduction

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

2. Operational and Logistic Measures

a. 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 C2 arrangements.

b. Employ force dispositions and C2 control arrangements that conceal the location, identity, and command relationships of major units.

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

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

e. Operate aircraft at low altitude to avoid radar detection.

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

g. Use darkness to mask deployments or force generation.

h. Approach an objective "out of the sun" to prevent detection.

3. Technical Measures

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

b. Prepare for computer network attack. Place vital operational information on disk.

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

d. 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, landline, and couriers. Limit use of high frequency radios and directional super-high frequency transponders.

e. 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.

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

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

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

4. Administrative Measures

a. Limit non-secure telephone conversation with nonmilitary activities.

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

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

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

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

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

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

5. Operations Security and Military Deception

a. OPSEC used in conjunction with MILDEC can assist commanders to protect key elements of operations and ensure mission success. OPSEC, with MILDEC, can be used to facilitate the following:

(1) 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.

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

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

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

b. In accordance with JP 3-58, *Military Deception*, commanders are authorized to conduct MILDEC:

(1) 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.

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

6. Operations Security, Physical Destruction, 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.

Intentionally Blank

APPENDIX D
PROCEDURES FOR OPERATIONS SECURITY ASSESSMENTS

Annex A Operations Security Assessment Planning Phase
B Field Assessment Phase
C Analysis and Reporting Phase

PROCEDURES FOR OPERATIONS SECURITY ASSESSMENTS

1. General

a. The purpose of an OPSEC assessment is to thoroughly examine an operation or activity to determine if adequate protection from adversary intelligence exploitation exists.

b. Ideally, the operation or activity being assessed uses OPSEC measures to protect its critical information. The OPSEC assessment is used to verify the effectiveness of OPSEC measures. The assessment will determine if critical information identified during OPSEC planning process is being protected.

c. 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.

2. Uniqueness

a. 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.

b. In combat, an assessment's emphasis must be on identifying operational indicators that signal friendly intentions, capabilities, and/or limitations and that permit the adversary to counter friendly operations or reduce their effectiveness.

c. In peacetime, assessments generally seek to correct weaknesses that disclose information useful to potential adversaries in the event of future conflict. Many activities, such as operational unit tests, 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 long-range planning.

3. Operations Security Assessments Versus Security Inspections

a. 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.

b. 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.

c. 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.

d. 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.

e. To obtain accurate information, an assessment team must depend on 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.

f. 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.

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

4. Types of Assessments

There are two basic kinds of OPSEC assessments: command and formal.

a. A command assessment is performed using only command personnel and concentrates on events within the particular command.

b. A formal assessment requires an assessment team composed of members from inside and outside the command and will normally cross command lines (after prior coordination) to assess supporting and related operations and activities. Formal assessments are initiated by a letter or message stating the subject of the assessment, naming the team leader and members, and indicating when the assessment will be conducted. Commands, activities, and locations to be visited may also be listed, with the notation that the team may visit additional locations if required during the field portion of the assessment.

c. Both types of assessments follow the same basic sequence and procedures that are established in the annexes to this appendix.

5. Assessment Execution

a. Careful prior planning, thorough data collection, and thoughtful analysis of the results are the key phases of an effective OPSEC assessment.

b. The following annexes describe the three phases of an OPSEC assessment.

ANNEX A TO APPENDIX D
OPERATIONS SECURITY ASSESSMENT PLANNING PHASE

Tab A Functional Outline and Profile Guideline for Intelligence Collection Operations
B Functional Outline and Profile Guideline for Logistics
C Functional Outline and Profile Guideline for Communications
D Functional Outline and Profile Guideline for Operations
E Functional Outline and Profile Guideline for Administration and Support

OPERATIONS SECURITY ASSESSMENT PLANNING PHASE

1. Introduction

Preparations for an OPSEC assessment begin well in advance of the field assessment phase. The required lead time will depend 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.

2. 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.

3. Select Team Members

a. 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.

b. 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.

c. Typical team members would represent the functional areas of intelligence (to include counterintelligence), security, communications, logistics, plans, IA, PA, 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.

4. 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.

5. Determine the Adversary Intelligence Threat

The adversary threat to the activities to be assessed is evaluated carefully and realistically. An all-source threat assessment should comprehensively address the adversary intelligence capability, taking into account the adversary's collection capabilities and the adversary's ability to exploit the collection results in a timely manner.

6. 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, 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).

7. Conduct Empirical Studies

a. Empirical studies 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.

b. An example of an empirical study is signals monitoring. Computer modeling or other laboratory simulations of the adversary threat, the impact on friendly forces, and the impact of implementing defensive measures may also be useful to the assessment team. These studies are usually performed by organizations external to the one sponsoring the OPSEC assessment team. Arrangements for their use should be made as far in advance of the assessment as possible.

8. Develop a Functional Outline

a. 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.

b. Chronologies should first be constructed for each separate functional area, such as operations, communications, logistics, or administration. This functional approach aids the team members in defining their separate areas of inquiry during the field or data collection phase of the assessment. Later, the functional outlines can be correlated with each other to build an integrated chronology of the entire operation or activity.

c. After the chronology is assembled, vulnerabilities can be identified in light of the known or projected threat.

d. During the initial review of OPLANs, OPORDs, and SOPs, individual team members can begin to develop functionally oriented outlines for their areas of interest. Initially, the outlines are skeletal projections, in a narrative, table, or graph format, of what is expected to occur in the chronology for a particular functional area (see Tabs B through E).

e. Such projections can serve as planning aids for the subsequent field assessment phase. For example, units and facilities associated with each of the events are identified and geographically grouped to aid in planning the travel itinerary of team members during the field

assessment. Collectively, the initial functional outlines provide a basis for planning the field assessment phase and constitute a basis for observation and interviews.

f. During the field assessment phase, team members will acquire additional information through observation, interviews, and other data-collection techniques, enabling further development and refinement of the functional outlines.

g. 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.

9. 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.

10. Announce the Assessment

a. 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.

b. The following information should be included:

(1) Assessment purpose and scope.

(2) List of team members and their clearances.

(3) List of required briefings and orientations.

(4) Timeframe involved.

(5) Administrative support requirements.

(6) All support requirements, such as signal security (SIGSEC) monitoring support requirements (if needed).

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

TAB A TO ANNEX A TO APPENDIX D
FUNCTIONAL OUTLINE AND PROFILE GUIDELINE FOR INTELLIGENCE COLLECTION OPERATIONS

1. **General.** The completed 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.

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

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

4. **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.

5. **Examples of Typical Indicators**

a. Appearance of specialized intelligence collection equipment in a particular area.

b. Increased traffic on intelligence communications nets.

c. Increased manning levels and/or work hours in intelligence facilities.

d. Increased research known intelligence activities and personnel in libraries and electronic databases.

e. Increased activity of friendly agent nets.

f. Increased levels of activity by airborne intelligence systems.

g. Alterations in the orbits of intelligence satellites.

h. Interviews with nongovernmental subject matter experts conducted by intelligence personnel.

i. Requests for maps and other topographic material.

j. Appearance of OPSEC assessment team.

Intentionally Blank

TAB B TO ANNEX A TO APPENDIX D
FUNCTIONAL OUTLINE AND PROFILE GUIDELINE FOR LOGISTICS

1. **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.

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

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

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

5. **Examples of Typical Indicators**

a. Special equipment issue.

b. Pre-positioning of equipment and supplies.

c. Increased weapons and vehicle maintenance.

d. Petroleum, oils, and lubricants stockpiling.

e. Upgrading lines of communications.

f. Ammunition stockpiling.

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

h. Arrival of new logistic units and personnel.

i. Increased requisition of supplies.

j. Increased traffic on logistic communications nets.

k. Changes in normal delivery patterns.

l. Appearance of OPSEC assessment team.

Intentionally Blank

TAB C TO ANNEX A TO APPENDIX D
FUNCTIONAL OUTLINE AND PROFILE GUIDELINE FOR COMMUNICATIONS

1. **General.** In addition to presenting 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.

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

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

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

5. **Examples of Typical Indicators**

   a. Increased radio, teletype, and telephone traffic.

   b. Increased communications checks.

   c. Appearance of new stations in net.

   d. New frequency and call-sign assignments.

   e. New codes and authenticators.

   f. Radio silence.

   g. Changing callup patterns.

   h. Use of maintenance frequencies to test equipment.

   i. Communications command post exercises.

   j. Appearance of different cryptographic equipment and materials.

   k. Unclassified network activity.

   l. Appearance of OPSEC assessment team.

Intentionally Blank

TAB D TO ANNEX A TO APPENDIX D
FUNCTIONAL OUTLINE AND PROFILE GUIDELINE FOR OPERATIONS

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

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

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

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

5. **Examples of Typical Indicators**

a. Rehearsals and drills.

b. Special-tactics refresher training.

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

d. Pre-positioning of artillery and aviation units.

e. Artillery registration in new objective area.

f. Complete cessation of activity in area in which reconnaissance activity previously took place.

g. Appearance of new attached units.

h. Issuance of new equipment.

i. Changes in major unit leadership.

j. Repositioning of maneuver units.

k. Appearance of OPSEC assessment team.

Intentionally Blank

TAB E TO ANNEX A TO APPENDIX D
FUNCTIONAL OUTLINE AND PROFILE GUIDELINE FOR ADMINISTRATION AND SUPPORT

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

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

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

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

5. **Examples of Typical Indicators**

   a. Release of groups of personnel or complete units for personal affairs.

   b. Runs on exchanges for personal articles, cleaning, and other items.

   c. Changes to wake-up and dining schedules.

   d. Changes to mailing addresses.

   e. New unit designators on mail.

   f. Emergency personnel requisitions and fills for critical skills.

   g. Medical supply stockpiling.

   h. Emergency recall of personnel on pass and leave.

   i. Appearance of OPSEC assessment team.

Intentionally Blank

ANNEX B TO APPENDIX D
FIELD ASSESSMENT PHASE

1. Introduction

As noted previously, data collection begins in the planning phase with a review of associated documentation. During the field 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 field assessment phase.

2. 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.

3. 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.

4. Data Collection and Functional Outline Refinement

a. **Data Collection**

(1) During the field 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 SIGSEC 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 persons 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.

b. **Functional Outline Refinement**

(1) As indicated earlier, each team member should have a basic functional outline to direct data collection efforts at the beginning of the field assessment phase. The basic outline is modified during this phase to reflect new information obtained by observation and interview and will ultimately become a profile of actual events.

(2) Each team member should be familiar with the outlines used by the other members of the assessment team and should be alert for information that might affect them. An interview in the communications area, for example, might disclose information that would result in a change to the outline being developed for operations; or an observation in one geographic location could affect an outline being followed up in another. Also, to permit followup elsewhere, all outlines should try to reflect the information generated and the flow at each location where data is collected.

(3) As data is accumulated through observation and interviews, incorporation of such data into the basic functional outline changes the original list of projected events into a profile of actual events. The functional outline then becomes a chronological record of what actually was done, where, who did it, and how and why it was done. The outline should also reflect an assessment of the vulnerability of each event to the known or suspected hostile intelligence 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 field 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 field assessment phase. Final development and production of the assessment report can then proceed immediately upon the team's return to home station.

5. Team Employment

a. 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.

b. It is rarely possible, however, to plan employment in detail before the field 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.

c. The duration of the field assessment phase is established during the planning phase and depends on how rapidly data is collected. Many assessments have required 30 days or more in the field. 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 field assessment phase.

6. Operations Security Assessment Team Exit Briefing

a. 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.

b. 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.

c. 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.

ANNEX C TO APPENDIX D
ANALYSIS AND REPORTING PHASE

Tab A Example Format for Final Operations Security Assessment Report

ANALYSIS AND REPORTING PHASE

1. Introduction

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

2. Correlation of Data

a. **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.

b. **Functional Outlines.** The purpose of constructing the functional outlines is to describe the time-phased progression of the operation or activity; to depict the manner in which separate commands, organizations, and activities interact and perform their roles in the operation or activity; and to trace the flow of information through electrical and nonelectrical communications media from its origin to its ultimate recipients. It is important that the team members present the information in a manner that facilitates analysis. The net result of the correlation will be a portrayal of the entire operation or activity.

c. **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 importantly, these data can also verify vulnerabilities that would otherwise be exceedingly speculative or tenuous. Empirical data is extremely important to a comprehensive assessment.

3. Identification of Vulnerabilities

a. 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.

b. 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.

c. 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.

4. Operations Security Assessment Report

a. 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.

b. The format for OPSEC assessment reports is found in Tab A, "Example Format for Final Operations Security Assessment Report." The report should provide a discussion of identified critical information, indicators, adversaries and their intelligence capabilities, OPSEC vulnerabilities, risk analysis, and recommended OPSEC measures 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.

c. 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.

d. 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.

e. 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 where 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.

f. 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.

g. 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.

h. 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.

i. 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.

TAB A TO ANNEX C TO APPENDIX D
EXAMPLE FORMAT FOR FINAL OPERATIONS SECURITY ASSESSMENT REPORT

1. Overview

a. Background. Address the purpose and scope of the assessment as well as the results of the threat and vulnerability assessments.

b. Conduct of Assessment. Brief discussion of methodology, team composition, major commands visited, and timeframe of assessment.

c. Critical Information.

d. Threat.

2. Summary of Significant Findings

3. Analysis, Conclusions, and Findings

This is the body of the report. Discussions and findings may be listed chronologically, by command, or chronologically within commands.

4. The Suggested Format for Each Finding

a. Observation.

b. Analysis and discussion.

c. Conclusion or recommendation.

Intentionally Blank

APPENDIX E
REFERENCES

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

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

2. CJCSI 3210.03B, *Joint Electronic Warfare Policy*.

3. CJCSI 3211.01C, *Joint Policy for Military Deception*.

4. CJCSI 3213.01B, *Joint Operations Security*.

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

6. CJCSI 5120.02, *Joint Doctrine Development System*.

7. CJCSM 3122.03A, *Joint Operation Planning and Execution System, Volume II, Planning Formats and Guidance.*

8. CJCSM 5714.01B, *Policy for Release of Joint Information*.

9. JP 1, *Joint Warfare of the Armed Forces of the United States*.

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

11. JP 2-0, *Doctrine for Intelligence Support to Joint Operations.*

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

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

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

15. JP 3-13.2, *Psychological Operations.*

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

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

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

Intentionally Blank

APPENDIX F
ADMINISTRATIVE INSTRUCTIONS

1. User Comments

Users in the field are highly encouraged to submit comments on this publication to: Commander, United States Joint Forces Command, Joint Warfighting Center, ATTN: Doctrine and Education Group, 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).

3. Supersession

This publication supersedes JP 3-54, 24 January 1997, *Joint Doctrine for Operations Security*.

4. Change Recommendations

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

TO: JOINT STAFF WASHINGTON DC//J3//DDIO
INFO: JOINT STAFF WASHINGTON DC//J7-JEDD//
CDRUSJFCOM SUFFOLK VA//DOC GP//

Routine changes should be submitted electronically to Commander, Joint Warfighting Center, Doctrine and Education Group and info the Lead Agent and the Director for Operational Plans and Joint Force Development J-7/JEDD via the CJCS JEL at http://www.dtic.mil/doctrine.

b. When a Joint Staff directorate submits a proposal to the Chairman of the Joint Chiefs of Staff 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 Military Services and other organizations are requested to notify the Joint Staff/J-7 when changes to source documents reflected in this publication are initiated.

c. Record of Changes:

CHANGE NUMBER	COPY NUMBER	DATE OF CHANGE	DATE ENTERED	POSTED BY	REMARKS

5. Distribution of Printed Publications

a. Additional copies of this publication can be obtained through the Service publication centers listed below (initial contact) or USJFCOM in the event that the joint publication is not available from the Service.

b. Individuals and agencies outside the combatant commands, Services, Joint Staff, and combat support agencies are authorized to receive only approved joint publications and joint test publications. Release of any classified joint publication to foreign governments or foreign nationals must be requested through the local embassy (Defense Attaché Office) to DIA Foreign Liaison Office, PO-FL, Room 1E811, 7400 Defense Pentagon, Washington, DC 20301-7400.

c. Additional copies should be obtained from the Military Service assigned administrative support responsibility by DOD Directive 5100.3, 15 November 1999, *Support of the Headquarters of Unified, Specified, and Subordinate Joint Commands*.

By Military Services:

Army:	US Army AG Publication Center SL 1655 Woodson Road Attn: Joint Publications St. Louis, MO 63114-6181
Air Force:	Air Force Publications Distribution Center 2800 Eastern Boulevard Baltimore, MD 21220-2896
Navy:	CO, Naval Inventory Control Point 700 Robbins Avenue Bldg 1, Customer Service Philadelphia, PA 19111-5099
Marine Corps:	Commander (Attn: Publications) 814 Radford Blvd, Suite 20321 Albany, GA 31704-0321
Coast Guard:	Commandant (G-OPD) US Coast Guard 2100 2nd Street, SW Washington, DC 20593-0001

Commander
USJFCOM JWFC Code JW2102
Doctrine and Education Group (Publication Distribution)
116 Lake View Parkway
Suffolk, VA 23435-2697

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

6. Distribution of Electronic Publications

a. The Joint Staff will not print copies of electronic joint publications for distribution. Electronic versions are available at www.dtic.mil/doctrine (NIPRNET), or http://nmcc20a.nmcc.smil.mil/dj9j7ead/doctrine/ (SIPRNET).

b. Only approved joint publications and joint test publications are releasable outside the combatant commands, Services, and Joint Staff. Release of any classified joint publication to foreign governments or foreign nationals must be requested through the local embassy (Defense Attaché Office) to DIA Foreign Liaison Office, PO-FL, Room 1E811, 7400 Defense Pentagon, Washington, DC 20301-7400.

Intentionally Blank

GLOSSARY

PART I — ABBREVIATIONS AND ACRONYMS

C2	command and control
CCDR	combatant commander
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
COA	course of action
COMSEC	communications security
CONPLAN	operation plan in concept format
DIA	Defense Intelligence Agency
DOD	Department of Defense
EEFI	essential elements of friendly information
IA	information assurance
IO	information operations
IOSS	Interagency Operations Security (OPSEC) Support Staff
J-3	operations directorate of a joint staff
J-7	Operational Plans and Joint Force Development Directorate, Joint Staff
JFC	joint force commander
JIOC	joint information operations center
JLLP	Joint Lessons Learned Program
JP	joint publication
JPG	joint planning group
LEA	law enforcement agency
MILDEC	military deception
NSA	National Security Agency
OEG	operations security (OPSEC) executive group
OPLAN	operation plan
OPORD	operation order
OPSEC	operations security
PA	public affairs
PAO	public affairs officer

SIGINT	signals intelligence
SIGSEC	signal security
SOP	standard operating procedure
WAN	wide-area network

PART II — TERMS AND DEFINITIONS

command and control. The exercise of authority and direction by a properly designated commander over assigned and attached forces in the accomplishment of the mission. Command and control functions are performed through an arrangement of personnel, equipment, communications, facilities, and procedures employed by a commander in planning, directing, coordinating, and controlling forces and operations in the accomplishment of the mission. Also called C2. (JP 1-02)

communications security. The protection resulting from all measures designed to deny unauthorized persons information of value that might be derived from the possession and study of telecommunications, or to mislead unauthorized persons in their interpretation of the results of such possession and study. Also called COMSEC. (JP 1-02)

computer network attack. Actions taken through the use of computer networks to disrupt, deny, degrade, or destroy information resident in computers and computer networks, or the computers and networks themselves. Also called CNA. (JP 1-02)

computer network operations. Comprised of computer network attack, computer network defense, and related computer network exploitation enabling operations. Also called CNO. (JP 1-02)

critical information. Specific facts about friendly intentions, capabilities, and activities vitally needed by adversaries for them to plan and act effectively so as to guarantee failure or unacceptable consequences for friendly mission accomplishment. (JP 1-02)

deception. Those measures designed to mislead the enemy by manipulation, distortion, or falsification of evidence to induce the enemy to react in a manner prejudicial to the enemy's interests. (JP 1-02)

electronic warfare. Any military action involving the use of electromagnetic and directed energy to control the electromagnetic spectrum or to attack the enemy. Also called EW. The three major subdivisions within electronic warfare are: electronic attack, electronic protection, and electronic warfare support. a. electronic attack. That division of electronic warfare involving the use of electromagnetic energy, directed energy, or antiradiation weapons to attack personnel, facilities, or equipment with the intent of degrading, neutralizing, or destroying enemy combat capability and is considered a form of fires. Also called EA. EA includes: 1) actions taken to prevent or reduce an enemy's effective use of the electromagnetic spectrum, such as jamming and electromagnetic deception, and 2) employment of weapons that use either electromagnetic or directed energy as their primary destructive mechanism (lasers, radio frequency weapons, particle beams). b. electronic protection. That division of electronic warfare involving passive and active means taken to protect personnel, facilities, and equipment from any effects of friendly or enemy employment of electronic warfare that degrade, neutralize, or destroy friendly combat capability. Also called EP. c. electronic warfare support. That division of electronic warfare involving actions tasked by, or under

direct control of, an operational commander to search for, intercept, identify, and locate or localize sources of intentional and unintentional radiated electromagnetic energy for the purpose of immediate threat recognition, targeting, planning and conduct of future operations. Thus, electronic warfare support provides information required for decisions involving electronic warfare operations and other tactical actions such as threat avoidance, targeting, and homing. Also called ES**.** Electronic warfare support data can be used to produce signals intelligence, provide targeting for electronic or destructive attack, and produce measurement and signature intelligence. (JP 1-02)

emission control. The selective and controlled use of electromagnetic, acoustic, or other emitters to optimize command and control capabilities while minimizing, for operations security: a. detection by enemy sensors; b. mutual interference among friendly systems; and/or c. enemy interference with the ability to execute a military deception plan. Also called EMCON. (JP 1-02)

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

operations security. A process of identifying critical information and subsequently analyzing friendly actions attendant to military operations and other activities to: a. identify those actions that can be observed by adversary intelligence systems; b. determine indicators that adversary intelligence systems might obtain that could be interpreted or pieced together to derive critical information in time to be useful to adversaries; and c. select and execute measures that eliminate or reduce to an acceptable level the vulnerabilities of friendly actions to adversary exploitation. Also called OPSEC. (This term and its definition modify the existing term and its definition and are approved for inclusion in the next edition of 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)

operations security measures. Methods and means to gain and maintain essential secrecy about critical information. (This term and its definition modify the existing term and its definition and are approved for inclusion in the next edition of JP 1-02.)

operations security planning guidance. Guidance that serves as the blueprint for operations security planning by all functional elements throughout the organization. It defines the critical information that requires protection from adversary appreciations, taking into account friendly and adversary goals, estimated key adversary questions, probable adversary knowledge, desirable and harmful adversary appreciations, and pertinent intelligence system threats. It also should outline provisional operations security measures to ensure the requisite essential secrecy. (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 decisionmaking. (JP 1-02)

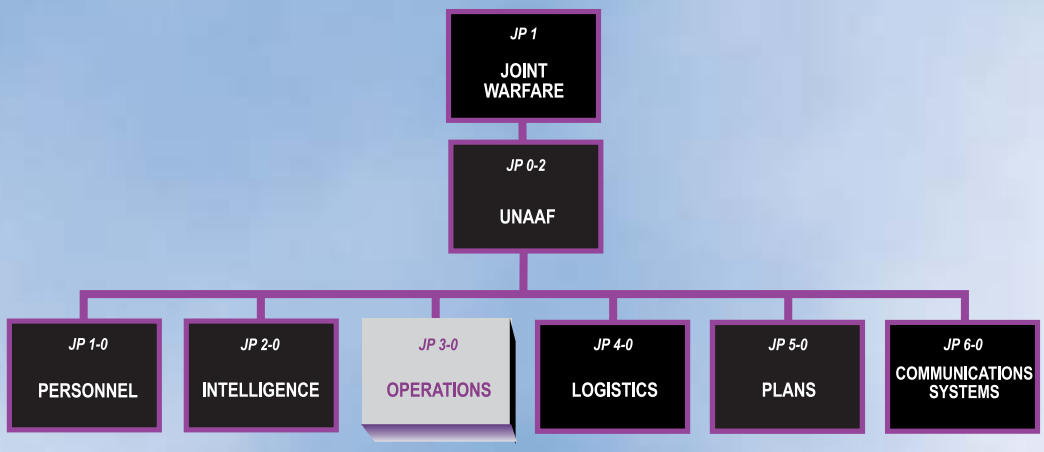
psychological operations. Planned operations to convey selected information and indicators to foreign audiences to influence their emotions, motives, objective reasoning, and ultimately the behavior of foreign governments, organizations, groups, and individuals. The purpose of psychological operations is to induce or reinforce foreign attitudes and behavior favorable to the originator's objectives. Also called PSYOP. (JP 1-02)

public affairs. Those public information, command information, and community relations activities directed toward both the external and internal publics with interest in the Department of Defense. Also called PA. (JP 1-02)

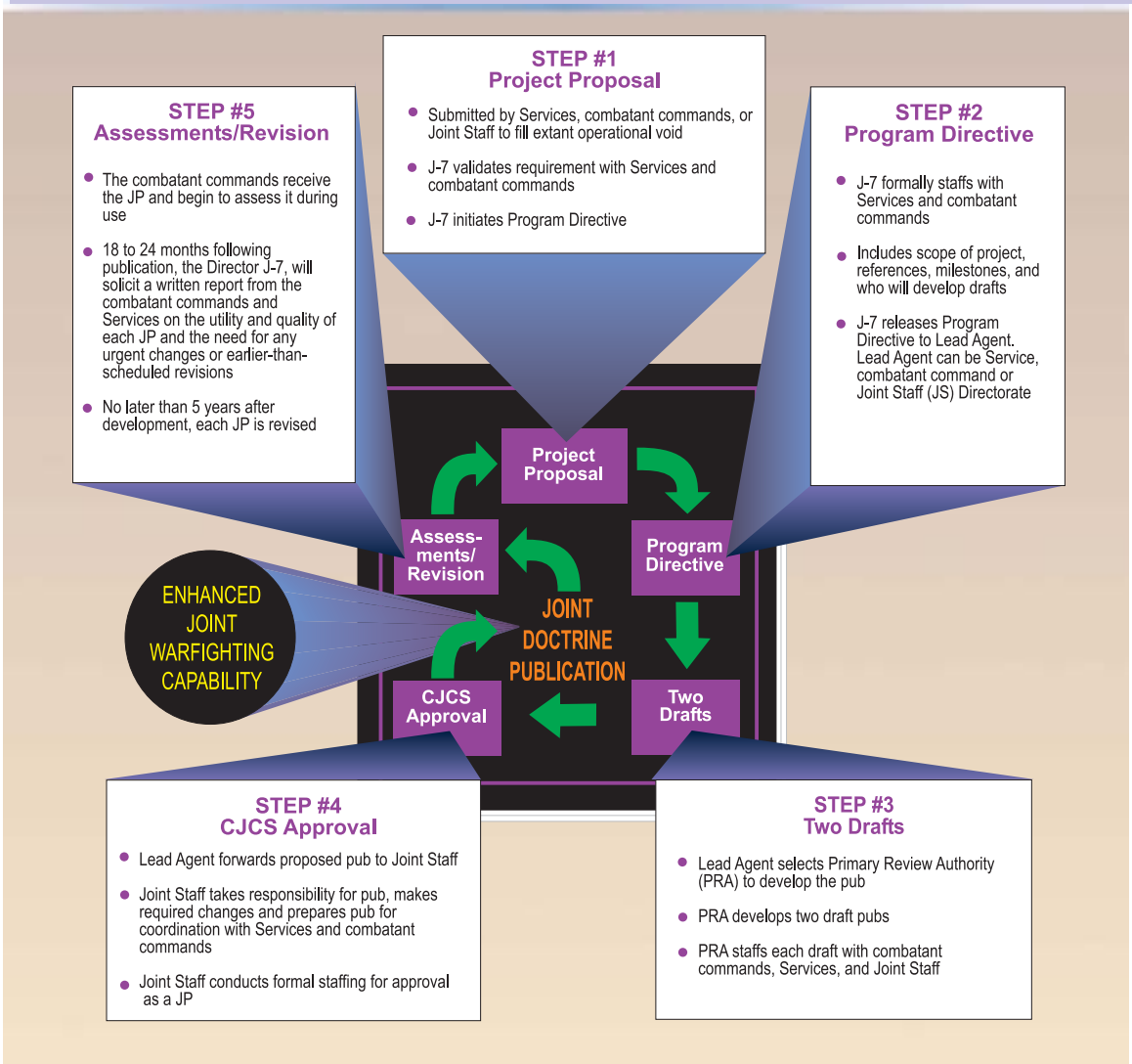
signal security. A generic term that includes both communications security and electronics security. (JP 1-02)

Intentionally Blank

JOINT DOCTRINE PUBLICATIONS HIERARCHY



All joint doctrine and tactics, techniques, and procedures 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:




JOINT
CHIEFS OF STAFF