Joint Publication 3-13.3

Operations Security

06 January 2016

PREFACE

1. Scope

This publication provides joint doctrine to plan, execute, and assess operations security within joint operations and activities.

2. Purpose

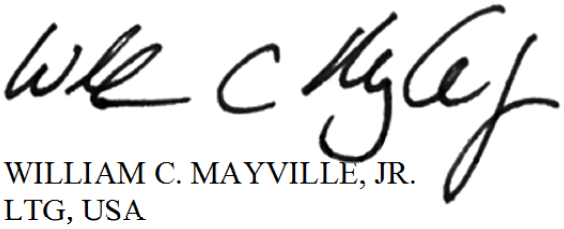
This publication has been prepared under the direction of the Chairman of the Joint Chiefs of Staff. It sets forth joint doctrine to govern the activities and performance of the Armed Forces of the United States in joint operations, and it provides considerations for military interaction with governmental and nongovernmental agencies, multinational forces, and other interorganizational partners. 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 and executing their plans and orders. 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 objectives.

3. Application

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

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 US, commanders should evaluate and follow the multinational command's doctrine and procedures, where applicable and consistent with US law, regulations, and doctrine.

For the Chairman of the Joint Chiefs of Staff:



WILLIAM C. MAYVILLE, JR.
LTG, USA
Director, Joint Staff

Intentionally Blank

SUMMARY OF CHANGES
REVISION OF JOINT PUBLICATION 3-13.3
DATED 04 JANUARY 2012

- **Restructures document format, rearranging information within chapters for better sequencing and flow while reducing redundancy.**

- **Updates definitions of operations security (OPSEC) and OPSEC indicators.**

- **Adds section in OPSEC overview on cyberspace, highlighting the key vulnerabilities associated with Internet use, to include social media, geotagging, data mining, and posting of contracting information on the Internet.**

- **Adds OPSEC planner to OPSEC responsibilities section, stressing the importance a trained OPSEC planner will have on protecting both the plan and the planning process.**

- **Adds quantitative and qualitative examples of both measurement of effectiveness and measurement of performance during the application of OPSEC countermeasures.**

- **Adds combatant command red teams as a factor to consider employing to support OPSEC planning, execution, and assessment.**

- **Expands on the relationship between OPSEC and military deception during the planning process and defines the use of deception in support of OPSEC as an OPSEC countermeasure.**

- **Restructures OPSEC assessment planning, execution, and analysis and reporting sections and adds Department of Defense 5205.02-M, *DOD Operations Security (OPSEC) Program Manual*, as reference for the conduct of OPSEC assessments and surveys, ensuring consistency in annual assessments.**

- **Updates Appendix C, "Sample Operations Security Plan," to reflect currency with Chairman of the Joint Chiefs of Staff Manual 3130.03, *Adaptive Planning and Execution (APEX) Planning Formats and Guidance*.**

- **Updates references, acronyms, and terminology consistent with other joint doctrine.**

Intentionally Blank

TABLE OF CONTENTS

APPENDIX

GLOSSARY

FIGURE

EXECUTIVE SUMMARY
COMMANDER'S OVERVIEW

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

Operations Security Overview

Operational Context

Joint forces often display personnel, organizations, assets, and actions to public view and to a variety of adversary intelligence collection activities, including sensors and systems.

Commanders ensure operational security (OPSEC) is practiced during all phases of operations. OPSEC is a capability that identifies and controls critical information, indicators of friendly force actions attendant to military operations, and incorporates countermeasures to reduce the risk of an adversary exploiting vulnerabilities.

As adversary analysts apply more information to an analytical model, the likelihood increases that the analytical model will replicate the observed force. Thus, current and future capabilities and courses of action can be revealed and compromised.

The purpose of operations security (OPSEC) is to reduce the vulnerability of US and multinational forces to successful adversary exploitation of critical information.

The OPSEC process is a systematic method used to identify, control, and protect critical information to:

- Identify actions that may be observed by adversary intelligence systems.
- Determine what specific indications could be collected, analyzed, and interpreted to derive critical information in time to be useful to adversaries.

- Select countermeasures that eliminate or reduce vulnerability or indicators to observation and exploitation.

- Preserve a commander's decision cycle and allow options for military actions.

OPSEC and Intelligence

Tailored to the OPSEC process, joint intelligence preparation of the operational environment is a useful methodology for intelligence professionals to support the OPSEC planner.

Characteristics of OPSEC

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

OPSEC and Information Operations

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

OPSEC and Cover

The important distinction between OPSEC and cover is that OPSEC denies information without misrepresenting it; cover misrepresents information.

OPSEC and Cyberspace

OPSEC officers, in coordination with the public affairs officer and cybersecurity personnel, should review their command's presence on the World Wide Web through the eyes of the adversary.

Only information of value to the general public and that does not require additional protection should be posted to publicly accessible sites on the Internet.

OPSEC Responsibilities

Chairman of the Joint Chiefs of Staff advises the Secretary of Defense concerning OPSEC support to the combatant commands (CCMDs) and is responsible for providing joint OPSEC policy and doctrine.

Joint Staff J-3, Director of Operations, executes primary Joint Staff responsibility for OPSEC and supports OPSEC planning and training by the Joint Staff, Services, CCMDs, and Department of Defense agencies.

Service Chiefs provide Service OPSEC policy, doctrine, and planning procedures and OPSEC-related training to all Service members.

Combatant commanders provide OPSEC guidance for all operations, exercises, and other joint activities of the command; plan for and execute OPSEC countermeasures in support of assigned missions.

The Operations Security Process

The OPSEC process consists of five steps or elements.

Identify Critical Information. Critical information answers key questions likely to be asked by adversaries about specific friendly intentions, capabilities, and activities.

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

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

Risk assessment has three components: analyze the vulnerabilities and identify possible OPSEC countermeasures; estimate the impact to operations; and select specific OPSEC countermeasures for execution

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

Operations Security Planning

OPSEC Factors

Because OPSEC is an operations function, not a security function, OPSEC planning guidance should be provided as part of the commander's planning guidance and applied throughout the planning process.

Attempting to deny all information about a friendly operation or activity is seldom cost-effective or realistic.

OPSEC planning should emphasize protection of critical information before, during, and after operations.

OPSEC indicators are continuously analyzed and considered during planning.

There are five major indicator characteristics:

Signature is a characteristic that makes an action or piece of information identifiable or causes it to stand out. Key signature properties are uniqueness and stability.

Associations are the relationships of an indicator to other information or activities. It is an important key to an adversary's interpretation of ongoing activity.

A profile is the sum of unique signatures and associations of a functional activity.

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.

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.

OPSEC Countermeasures

Development of specific OPSEC countermeasures is as varied as the specific vulnerabilities they are designed to offset. Some considerations include operational and logistic countermeasures; technical countermeasures;

administrative countermeasures; as well as OPSEC and military deception.

Operations Security Assessments and Surveys

Assessments and Surveys

An OPSEC assessment is an intensive application of the OPSEC process to an existing operation or activity.

An OPSEC survey is conducted by a team of external subject matter experts from multiple disciplines to simulate adversary intelligence processes.

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.

CONCLUSION

This publication provides joint doctrine to plan, execute, and assess OPSEC within joint operations and activities.

Intentionally Blank

CHAPTER I
OPERATIONS SECURITY OVERVIEW

"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) 3213.01, *Joint Operations Security*.

2. Operational Context

a. Joint forces often display personnel, organizations, assets, and actions to public view and to a variety of adversary intelligence collection activities, including sensors and systems. Joint forces can be under observation at their peacetime bases and locations, in training or exercises, while moving, or when deployed conducting actual operations. The actions or behavior of military family members and businesses associated with or supporting military operations are also subject to observation by adversaries, which could equally be associated with activities or operations of the joint force. Frequently, when a force performs a particular activity or operation a number of times, it establishes a pattern of behavior. Within this pattern, certain unique, particular, or special types of information might be associated with an activity or operation. Even though this information may be unclassified, it can expose US military operations to observation and/or attack. Commanders ensure OPSEC is practiced during all phases of operations. OPSEC is a capability that identifies and controls critical information, indicators of friendly force actions attendant to military operations, and incorporates countermeasures to reduce the risk of an adversary exploiting vulnerabilities. In addition, the adversary could compile and correlate enough information to predict and counter US operations.

b. Commanders cannot limit their protection efforts to a particular operational area or threat. With continuing rapid advancement and global use of communications systems and information technology, easily obtainable technical collection tools, and the growing use of the Internet and various social and mass media outlets, the ability to collect critical information virtually from anywhere in the world and threaten US military operations continues to expand. To prevent or reduce successful adversary collection and exploitation of US critical information, the commander should formulate a prudent, practical, timely, and effective OPSEC program. Additionally, the commander's OPSEC program must establish, resource, and maintain formal OPSEC programs. The commander should formulate these OPSEC programs to be prudent, practical, timely, and effective.

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

d. Adversary intelligence personnel continuously analyze and interpret collected information to validate and/or refine the model. As adversary analysts apply more information to the analytical model, the likelihood increases that the analytical model will replicate the observed force. Thus, current and future capabilities and courses of action (COAs) can be revealed and compromised. **Critical information** consists of specific facts about friendly intentions, capabilities, and activities needed by adversaries to plan and act effectively so as to guarantee failure or unacceptable consequences for friendly mission accomplishment. Critical information can be either classified or unclassified.

e. OPSEC considerations must also be observed while working with interagency partners.

3. Purpose of Operations Security

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

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

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

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

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

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

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

(c) Avoid patterns of behavior, whenever feasible, to preclude the possibility of adversary intelligence constructing an accurate model.

(4) Preserve a commander's decision cycle and allow options for military actions.

c. OPSEC is a force multiplier that can maximize operational effectiveness by saving lives and resources when integrated into operations, activities, plans, exercises, training, and capabilities.

4. Operations Security and Intelligence

a. Intelligence plays a key role in the OPSEC process. Joint intelligence preparation of the operational environment (JIPOE) is the analytical process used by joint intelligence organizations to produce intelligence assessments, estimates, and other intelligence products in support of the joint force commander's (JFC's) decision-making process. JIPOE's main focus is to provide predictive intelligence designed to help the JFC discern the adversary's probable intent and most likely future COA. Tailored to the OPSEC process, JIPOE is a useful methodology for intelligence professionals to support the OPSEC planner.

b. The first step of JIPOE is to define the operational environment—operational areas and areas of interest. In the case of OPSEC and protecting unclassified critical information, the operational environment can be considerably larger where an adversary intelligence organization can collect on friendly activities. Also during this step, the intelligence professional analyzes the mission and JFC's intent. This provides great insight into potential areas where the adversary could collect information.

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

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

e. The fourth and final step of the JIPOE process is to determine the adversary's COAs. The purpose of step four is to identify the COA the adversary is most likely to adopt and the COA that would be most dangerous to the friendly force or to mission

accomplishment. In terms of OPSEC, this amounts to where the adversary will most likely deploy its resources to collect information on the friendly force.

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

5. Characteristics of Operations Security

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

b. Unlike security programs that seek to protect classified information and controlled unclassified information (CUI), OPSEC **identifies, controls, and protects unclassified critical information** that is associated with specific military operations and activities. While some of the critical information in an OPSEC program may be CUI, most of the critical information is situation dependent. **OPSEC and security programs must be closely coordinated** to ensure appropriate aspects of military operations are protected. OPSEC and other security programs (i.e., information security, physical security, personnel security, industrial security, acquisition security, emissions security, cybersecurity, communications security [COMSEC], etc.) are complementary and should not be confused as being the same.

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

6. Operations Security and Information Operations

OPSEC, as an information-related capability (IRC), denies the adversary the information needed to correctly assess friendly capabilities and intentions. It is also a tool, hampering the adversary's use of its own information systems and processes and providing the necessary support to all IRCs. OPSEC complements the other IRCs and should be integrated into planning. In particular, OPSEC complements military deception (MILDEC) by denying an adversary information required to both assess a real plan and to disprove a deception plan. OPSEC and MILDEC affect the adversary's decision-making process, which can lead to the adversary making an erroneous decision. OPSEC does it by concealing important information, and MILDEC does it by putting misleading information into the environment. These are two related processes. OPSEC and MILDEC planners, facilitated by the OPSEC program manager, synchronize within the information operations (IO) cell to develop deception in support of operations

security (DISO) plans. For capabilities that exploit new opportunities and vulnerabilities, such as electronic warfare and cyberspace operations, OPSEC is essential to ensure friendly capabilities that might be easily countered are not compromised. The process to identify critical information and apply 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, cybersecurity, and personnel programs that screen personnel and limit authorized access. In particular, COMSEC plays a vital role in OPSEC. While COMSEC's primary purpose is to protect classified materials, it can aid to identify vulnerabilities to the loss of critical information through monitoring communications within legal constraints.

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

7. Operations Security and Cover

OPSEC protects critical information without misrepresentation. Cover is the concealment of true identity or organizational affiliation with assertions of false information as part of, or in support of, official duties to carry out authorized activities and lawful operations. The important distinction between OPSEC and cover is that OPSEC denies information without misrepresenting it; cover misrepresents information. Whether it is used in conjunction with OPSEC or MILDEC, all cover must be authorized in an approved cover plan.

For more information refer to Department of Defense Directive (DODD) S-5205.61, (U) DOD Cover and Cover Support Activities.

8. Operations Security and Cyberspace

a. OPSEC officers, in coordination with the public affairs officer (PAO) and cybersecurity personnel, should review their command's presence on the World Wide Web through the eyes of the adversary, looking for critical information and indicators that may reveal sensitive operations, movement of certain assets, personal information about US citizens and employees, and technological data.

b. Only information of value to the general public and that does not require additional protection should be posted to publicly accessible sites on the Internet. Information requiring additional protection, such as FOUO [For Official Use Only], or information not specifically cleared and approved for public release poses an unacceptable risk and should only be placed on sites with security and access controls.

c. While the Internet provides a powerful tool to convey information quickly and efficiently to conduct daily activities, it also increases the vulnerability of the organization and employees. The particular problem posed by today's technology is that Internet connectivity provides a singular user with new and increasingly efficient tools for reviewing and compiling information. Through a variety of techniques, attackers can hijack a person's social network account to use as a launching pad for additional attacks against other users. Department of Defense (DOD) and other United States Government

(USG) departments and agencies are active on social networking sites. If the adversary can observe the same action carried out in the same way at the same time, then they can easily identify not only routine activities but deviations as well.

d. Today's data-mining capabilities enable individuals to collect information from any number of different sources and quickly compile them into a product that contains sensitive or controlled, and very possibly, classified information. Both state and non-state actors have proven effective at this technique. Geography is no longer a primary factor in information gathering, to select and develop knowledge about a target. Additionally, Internet search tools use algorithms, which may tie or aggregate sensitive information.

e. Geotagging on social networking sites is increasing in popularity. From virtual check-ins to simply uploading photos with geographical and time-stamped information included in the data, users are posting detailed physical location metadata online for the world to see. The technology for geotagging now comes standard on newer digital cameras and smartphones and is easily extracted with a simple software downloadable for free in many cases.

f. This means, information posted on websites may pose more risk than information about the organization and its mission that is available through other means. Using information obtained through the Internet, an adversary can quickly search the multiple sites and derive indicators that point to or ascertain the critical piece of information necessary to counter a mission or operation. Because of the increased risk that someone may piece together the information puzzle, small items of information posted on publicly accessible websites are of increased OPSEC significance. An OPSEC officer/planner can no longer simply review their activity on their websites for items that may be targets for an adversary, since there is no way of specifically identifying which items in conjunction with information from other sites or sources may become critical indicators.

g. OPSEC officers/planners should caution employees on what should or should not be posted on DOD publicly-accessible websites, personal websites, and social media outlets. Some information, such as locations of, and hazards from, storage sites within an area of interest may require approval prior to posting. Civil defense considerations must be balanced against providing targeting data to an adversary.

h. Contracts can and should contain OPSEC guidelines wherein the activity reviews and approves information prior to posting on the contractor's website to minimize inadvertent disclosure of critical information. An OPSEC solution to the possible security vulnerability is to adopt a zero-based approach to website content. Decide which items combined with other information would be critical to an outside collector. Use OPSEC procedures to determine what information is absolutely necessary to post on websites to fulfill the mission and do not post any other information. Below are the most important considerations in zero-based website security:

(1) Assess the benefits to be gained by posting specific types of information on a website. Identify a target audience for each type of information and why their need for

the information is important to the organization's mission. A careful examination of the potential consequences of placing information on the website is necessary.

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

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

(4) In the past, OPSEC focused on activities that may not have been seen by a human observer, a satellite, a radio intercept operator, or the media. With the proliferation of information technologies over the last three decades, the access to DOD data has grown exponentially. The old threats have not gone away, but there is a new area of concern that OPSEC officers and planners must consider—the Internet. A disciplined approach to information security procedures, in conjunction with the OPSEC process, will ensure CUI is properly protected.

9. Operations Security Responsibilities

a. **Chairman of the Joint Chiefs of Staff (CJCS).** The CJCS advises the Secretary of Defense concerning OPSEC support to the combatant commands (CCMDs). The CJCS is responsible for providing joint OPSEC policy and doctrine. The CJCS also provides guidance to the combatant commanders (CCDRs) for review and evaluation of their OPSEC programs. The CJCS provides procedures for OPSEC planning in the Adaptive Planning and Execution (APEX) enterprise and ensures appropriate OPSEC countermeasures are implemented during joint operations and exercises.

b. **Joint Staff J-3 [Director of Operations]**

(1) The Joint Staff J-3 executes primary Joint Staff responsibility for OPSEC, designates OPSEC staff positions for the Joint Staff, and provides OPSEC advocacy for the CCDRs. The Joint Staff J-3 provides guidance for input of OPSEC lessons learned into the Joint Lessons Learned Information System database. The Joint Staff J-3 supports OPSEC planning and training by the Joint Staff, Services, CCMDs, and DOD agencies.

(2) The Joint Staff J-3 maintains the Joint Operations Security Support Element (JOSE) to provide OPSEC training, program review, surveys, and plans and exercise support to the CCDRs.

(3) The Joint Staff J-3 coordinates with the Joint Staff J-5 [Director for Strategic Plans and Policy] to ensure OPSEC is adequately addressed and evaluated in planning. The Joint Staff J-3 coordinates with the Joint Staff J-7 [Director for Joint Force Development] to ensure OPSEC is adequately addressed and evaluated in training and exercises. The Joint Staff J-3 establishes the operations security executive groups

(OEGs), as necessary, composed of members of the Joint Staff, Services, and appropriate agencies, to address specific OPSEC issues, such as problems relating to OPSEC programs that involve multiple commands or agencies. The Joint Staff J-3 also coordinates with the National Security Agency's (NSA's) Interagency Operations Security Support Staff (IOSS) and the Defense Threat Reduction Agency for OPSEC support.

c. **Service Chiefs**

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

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

d. **CCDRs**

(1) CCDRs provide OPSEC guidance for all operations, exercises, and other joint activities of the command. CCDRs conduct OPSEC planning in accordance with applicable policy and plan for and execute OPSEC countermeasures in support of assigned missions. Many times, OPSEC requires CCDRs to actively communicate the significance and purpose of protecting information for personnel to understand impacts to the overall mission beyond the limited scope of an individual's assigned task or responsibility. They coordinate OPSEC countermeasures and their execution with JOSE or CCMDs and other commands and agencies of those activities that cross command boundaries and report any unresolved issues to the Joint Staff J-3 for assistance. CCDRs conduct OPSEC assessments and surveys in support of command operations; conduct OPSEC reviews; and identify areas requiring additional CJCS guidance, assistance, or clarification to the Joint Staff J-3. CCDRs also designate an OPSEC program manager in the command headquarters.

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

(3) As a force provider for special operations forces, Commander, United States Special Operations Command, through its OPSEC support element, provides direct support to ensure preparedness of theater special operations commands.

e. **Director, Defense Intelligence Agency (DIA).** The Director, DIA, establishes and maintains an OPSEC training program for DIA personnel (civilian, military, and contractor) and attendees at the National Intelligence University, designates an agency OPSEC program manager, and designates representatives to Joint Staff OEGs, as required. The Director, DIA, also identifies, reviews, and validates DIA and other DOD

threat assessment documents for Joint Staff use. The Director, DIA, conducts analysis of the foreign intelligence collection threat for required nations and organizations for use in OPSEC planning and for monitoring the effectiveness of implemented OPSEC countermeasures, and provides results to the CJCS, CCDRs, Service Chiefs, and heads of the DOD agencies.

f. **NSA's IOSS**

(1) NSA's IOSS assists DOD and others with a national security mission to establish OPSEC programs, usually through the joint or Service OPSEC support element, as requested. The Director, NSA, provides interagency OPSEC training courses and designates a representative to Joint Staff OEGs, as required.

(2) NSA collaborates with DOD components by providing:

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

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

(c) Communications and cybersecurity support for OPSEC surveys.

(d) SIGINT support for OPSEC threat development.

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

g. **OPSEC Program Manager.** The OPSEC program manager's primary function is to advise the Service Chief, CCDR, or other JFC as applicable on OPSEC matters and maintain the organization's OPSEC program, to include writing the organization's policy and guidance documents, and ensure OPSEC awareness and procedures are in place to control critical information and indicators. The OPSEC program manager manages the OPSEC working group to address specific OPSEC issues and monitor/promote OPSEC awareness. The OPSEC program manager also coordinates with appropriate intelligence, counterintelligence (CI) support, counterespionage, force protection, antiterrorism, security, and public affairs (PA) staff. They also coordinate with security program managers, and coordinate the development and integration of OPSEC with other IRCs.

h. **OPSEC Planner**. OPSEC planners synchronize the OPSEC plan with the OPSEC program manager's OPSEC program. They develop the OPSEC appendix to plans and orders as well as related OPSEC documents.

(1) Functions and responsibilities of OPSEC planners are to:

(a) Coordinate with intelligence providers to formulate threat collection assessments.

(b) Assist with the development of critical information lists (CILs).

(c) Develop and integrate OPSEC countermeasures to reduce vulnerabilities and indicators.

(d) Coordinate OPSEC surveys or assessments as necessary to identify vulnerabilities during operational planning and execution.

(2) Trained OPSEC planners should be used to integrate OPSEC with the joint operation planning process. In circumstances involving particularly complex operations, or operations requiring extraordinary security, it may be necessary to have dedicated OPSEC planners or create dedicated planning groups. When the planning level of effort is minimal or an OPSEC planner is not available, the OPSEC planning function may be performed by an OPSEC representative, such as an OPSEC program manager trained in planning, or a military planner trained in OPSEC. The JFC's OPSEC planner will follow guidance issued in CJCSI 3213.01, *Joint Operation Security*.

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

CHAPTER II
THE OPERATIONS SECURITY PROCESS

"No proceeding is better than that which you have concealed from the enemy until the time you have executed it. To know how to recognize an opportunity in war, and take it, benefits you more than anything else."

Machiavelli Dell'arte della guerra
— also known as On the Art of War (1520)

1. General

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

b. The OPSEC process is applicable across the range of military operations. Use of the process ensures that the resulting OPSEC countermeasures address all significant aspects of the particular situation and are balanced against operational requirements. OPSEC is a continuous process. The OPSEC process (Figure II-1) consists of five steps or elements: identification of critical information, analysis of threats, analysis of vulnerabilities, assessment of risk, and application of appropriate OPSEC countermeasures. These OPSEC actions are applied continuously during OPSEC planning. 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** consists of specific facts about friendly intentions, capabilities, and activities needed by adversaries to plan and act effectively against friendly mission accomplishment.

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

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

2. Identify Critical Information

a. **The identification of critical information focuses the remainder of the OPSEC process on protecting vital information** rather than attempting to protect all unclassified information. Critical information answers key questions likely to be asked

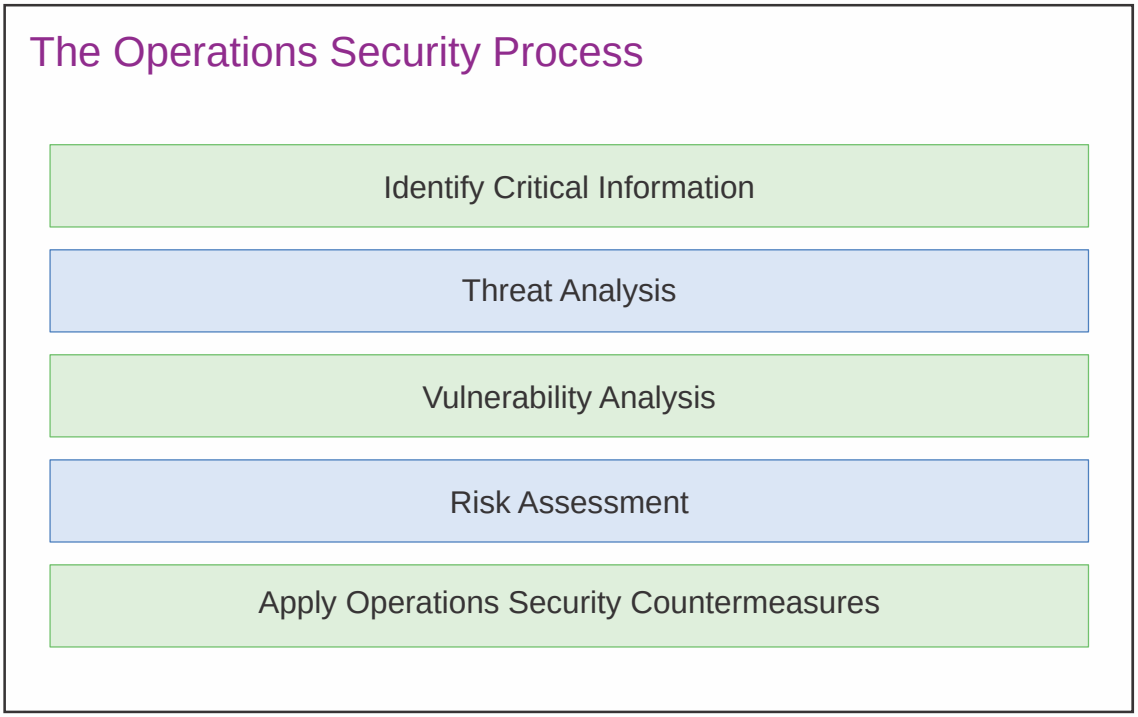


Figure II-1. The Operations Security Process

by adversaries about specific friendly intentions, capabilities, and activities. This information is necessary for adversaries to plan and act effectively against friendly mission accomplishment. There are many areas within an organization where elements of critical information can be obtained. Each section in an organization handles different information and it is vital all the critical information within the organization is protected. Additionally, personnel from outside the organization may also handle portions of its critical information. Therefore it is important to have personnel from each staff section and component involved in the process of identifying critical information. The critical information items should be consolidated into the CIL.

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

3. Threat Analysis

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

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

(1) Who is the adversary? What is his/her decision-making process? (Who has the intent and capability to take action against the planned operation?)

Examples of Critical Information

Notional Joint Operation Phases

Shape

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

Deter

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

Seize the Initiative

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

Dominate

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

Stabilize

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

Enable Civil Authority

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

Figure II-2. Examples of Critical Information

(2) What are the adversary's goals? (How does the information support his or her goals?)

(3) What is the adversary's most likely and most dangerous COA?

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

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

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

4. Vulnerability Analysis

a. The purpose of this action is to **identify an operation's or activity's vulnerabilities.** It requires examining each aspect of the planned operation to identify any OPSEC indicators or vulnerabilities that could reveal critical information and then comparing those indicators or vulnerabilities with the adversary's intelligence collection capabilities identified in the previous action. A vulnerability exists when the adversary is capable of collecting critical information, correctly analyzing it, and then taking timely action to exploit the vulnerability to obtain an advantage. Examples of vulnerabilities include observations of indicators, exploitation of open-source information (publications, trash, social media, and other Internet-based capabilities), unencrypted electronic mail (E-mail) and other communications, imagery, and elicitation.

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

(1) What critical information indicators are associated with the planned operation?

(2) What critical information or indicators can the adversary actually collect or observe?

(3) What indicators and vulnerabilities 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? Can the adversary exploit the information to conduct their own operation?)

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

5. Risk Assessment

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

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

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

(2) OPSEC countermeasures include encryption, concealment, camouflage, deception, intentional deviations from normal patterns, and direct strikes against the adversary's intelligence system. Each countermeasure, however, requires appropriate authorities and coordination prior to implementation by OPSEC personnel.

(3) **More than one possible countermeasure may be identified for each vulnerability.** Conversely, a single countermeasure may be used for more than one vulnerability. The most desirable OPSEC countermeasures are those that combine the highest possible protection with the least adverse effect on operational effectiveness.

Refer to Chapter III, "Operations Security Planning," for a detailed discussion of OPSEC countermeasures.

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

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

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

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

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

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

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

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

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

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

6. Apply Operations Security Countermeasures

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

b. A general OPSEC countermeasure strategy should be to:

(1) Minimize predictability from previous operations.

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

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

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

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

c. During planning, OPSEC personnel should establish measures of effectiveness (MOEs) and measures of performance (MOPs) to assess if the OPSEC objectives are being achieved.

(1) **MOE.** Monitor the adversary's reaction to determine the countermeasures' effectiveness and to provide feedback. Implementing OPSEC countermeasures should not reveal additional critical information. As a corollary, if the adversary identifies an OPSEC countermeasure that, in itself, may be enough to alert the adversary that a military operation is imminent. Examples of OPSEC MOEs:

(a) Quantitative MOEs

1. Reduction in the percentage of suspicious activity.

2. Reduction in the percentage of social engineering attempts.

3. Reduction in the number of elicitations.

4. Reduction in the number of tests of security.

(b) Qualitative MOEs

1. Lack of adversary reaction to mobilizations.

2. Adversary intelligence systems fail to detect critical operations, exercises, or other critical activities.

3. Adversary intelligence systems fail to properly analyze vital capabilities and characteristics of systems.

4. Adversary intelligence systems fail to detect radio and radar emissions.

(2) **MOP.** Provides OPSEC personnel a way to determine if OPSEC countermeasures are being properly implemented. Examples of OPSEC MOPs:

(a) Quantitative MOPs

1. Completion percentage of OPSEC training.

2. Number or percentage increase of social media websites monitored for content, including information within the CIL.

3. Percentage increase of units conducting trashcans inspection to identify inadvertent disclosure of CIL elements.

4. Increase in the number of spot checks to enforce credentials verification in controlled access areas.

5. Increase in number of units conducting OPSEC internal and external assessments.

6. Decrease in critical information found in unencrypted E-mails.

(b) Qualitative MOPs

1. Control of critical supplies (explosives, ammunition, military uniforms, and passes or badges).

2. Documents containing sensitive or controlled information are properly marked with appropriate security measures.

3. Personnel applying appropriate privacy settings on their social networking sites, especially not using geographic tagging on their social networking updates when traveling or deployed.

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

CHAPTER III
OPERATIONS SECURITY PLANNING

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

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

1. General

a. Many nations, organizations, and groups conduct active intelligence operations against the US and its Armed Forces. Open-source material and observations of US activities and operations are major sources of information for the adversary.

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

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

d. Equally important is protecting the planning process itself. A thorough plan can be defeated before planning is complete if an OPSEC plan is not created to protect the planning process. Similar to creating classification guidance, establishing an OPSEC plan to protect the plan informs all involved what needs to be protected.

2. Operations Security Factors

The following factors should be considered when conducting OPSEC planning:

a. **OPSEC planning guidance should be provided as part of the commander's planning guidance.** OPSEC should be included in the staff estimates and during the development of friendly COAs.

b. **OPSEC is an operations function, not a security function.** The OPSEC process is applied throughout the planning process and is performed by all planners, but especially the plans directorate of a joint staff and the operations directorate of a joint staff. Planners are assisted by the organization's OPSEC program manager and appropriate planners from other staff elements to integrate OPSEC and publish OPSEC guidance into all plans. Intelligence support, as early as possible in the planning process,

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

is particularly important in determining the threat to friendly operations, assessing friendly vulnerabilities, determining the adversary's capabilities, and predicting the adversary's COAs.

c. **OPSEC should be integrated into the IO cell.** The JFC's staff, which includes the IO cell, develops and promulgates guidance and plans for IO that are passed to the components, supporting organizations, and agencies for detailed planning and execution. The role of the OPSEC program manager is to facilitate OPSEC within the commander's plan. The OPSEC program manager coordinates CCMD or subordinate joint force OPSEC activities and coordinates with the communications systems directorate and other command organizations, as necessary, for NSA's joint communications security monitoring activity (JCMA) liaison. Close coordination between the MILDEC and OPSEC offices is critical as MILDEC and OPSEC can be mutually supportive when properly coordinated, but may be diametrically opposing when not properly coordinated.

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

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

f. **OPSEC is considered during the development and selection of friendly COAs.** COAs will differ in terms of how many OPSEC indicators will be created and how easily those indicators can be managed by OPSEC countermeasures. Depending

upon how important maintaining secrecy is to mission success, OPSEC considerations may be a factor in selecting a COA.

g. **OPSEC planning is a continuous process.**

(1) OPSEC must be included in all phases of an operation. OPSEC planning should emphasize protection of critical information before, during, and after operations. Operations in Iraq and Afghanistan have shown the dangers associated with the withdrawal of forces and the need to protect critical information to safeguard forces.

(2) Feedback on the success or failure of OPSEC countermeasures is evaluated based on MOEs, and the OPSEC plan is modified accordingly. Friendly intelligence and CI organizations, COMSEC monitoring assessments, and OPSEC assessments are the primary sources for feedback information and are continuous throughout the OPSEC planning process.

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

i. **The PAO coordinates with OPSEC planners** to provide assessments on the potential effects of media coverage and all other public release of information by members of the command. PAOs work closely with operations intelligence and risk management planners to develop guidelines to avoid inadvertent disclosure of sensitive information. They are involved in OPSEC planning, surveys, and security reviews to prevent the public release of critical information. PA planning should include considerations to reduce the time lag between an event and what can be communicated, as well as the coordination of OPSEC countermeasures and PA guidance. The PAO ensures military public information activities, including the media pool, media clearances, media releases, and authorization of video transmissions, are carried out within the established OPSEC countermeasures. The PAO also coordinates with the OPSEC program manager to ensure the command information program addresses OPSEC and ground rules for the release of information (officially or unofficially) by military members through the Internet and other communications mediums subject to public access or monitoring.

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

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

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

l. **OPSEC support is a core red team function.** CCMD red teams should be employed to support OPSEC planning, execution, and assessment. Red teams help staffs think critically and creatively in order to see OPSEC problems and potential solutions from alternative perspectives. Implicit tasks include proposing unorthodox, out-of-the-box assessments and COAs, countering organizational influences, analytical errors, human biases, and information gaps that might constrain or prejudice thinking; providing insight into the mindsets, perspectives, doctrines, cultural traits, and likely responses of the adversary and other relevant actors; and exploring potential unintended consequences, follow-on effects, and unseen opportunities and threats.

3. Operations Security Indicators

a. OPSEC indicators are continuously analyzed and considered during planning.

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

(1) **Signature**

(a) A signature is the characteristic of an indicator that makes it identifiable or causes it to stand out. Key signature properties are uniqueness and stability. Uncommon or unique features reduce the ambiguity of an indicator and minimize the number of other indicators that must be observed to confirm a single indicator's significance.

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

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

(2) **Associations**

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

(b) Another key association deals with continuity of actions, objects, or other indicators that may register as patterns to the observer or analyst. Such continuity

may not be the result of planned procedures but may result instead from repetitive practices or sequencing to accomplish a goal. If, for example, the intensive generation of aircraft sorties is always preceded by a maintenance standdown to increase aircraft readiness, detecting and observing the standdown may allow the adversary analyst or observer to predict the subsequent launch activity. Moreover, based on past patterns of the length of such standdowns, the analyst may be able to judge the scope of the sortie generation.

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

(3) **Profiles**

(a) A profile is the sum of unique signatures and associations of a functional activity. Each functional activity generates its own set of more-or-less unique signatures and associations. An activity's profile is usually unique. Given enough data, intelligence analysts can determine the profile of any activity. Most intelligence organizations seek to identify and record the profiles of their adversary's military activities and human factors.

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

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

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

(4) **Contrasts**

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

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

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

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

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

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

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

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

6. Who and at what level was the decision made regarding where, when, what, and how fighters and bombers will deploy? How is this compared to any previous deployments?

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

(5) **Exposure**

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

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

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

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

4. Operations Security Countermeasures

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

b. **Operational and Logistic Countermeasures**

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

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

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

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

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

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

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

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

(9) Physical Attack/Destruction, Cyberspace Attack, and Electronic Warfare (including electronic attack [EA]). During hostilities, use physical destruction, cyberspace attack, and EA against the adversary’s ability to collect and process information. Military actions that are used in support of OPSEC include strikes against an adversary’s satellites, SIGINT sites, radars, fixed sonar installations, reconnaissance aircraft, and ships.

For more information, see JP 3-09, Joint Fire Support*; JP 3-12,* Cyberspace Operations*; JP 3-13.1,* Electronic Warfare*; and JP 3-60,* Joint Targeting.

c. **Technical Countermeasures**

(1) Limit non-encrypted E-mail messages to nonmilitary activities. Do not provide operational information in non-encrypted E-mail messages.

(2) Defend against cyberspace threats by ensuring patches are installed in a timely manner, data is backed up to devices not connected to the network, and redundant communication means and procedures are in place.

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

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

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

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

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

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

d. **Administrative Countermeasures**

(1) Limit nonsecure telephone conversation with nonmilitary activities.

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

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

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

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

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

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

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

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

(10) Ensure adequate policy and procedures are in place for destroying documents through shredding, burning, or other approved method.

(11) Ensure proper storage is available for classified and sensitive or controlled unclassified material.

e. **OPSEC and MILDEC**

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

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

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

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

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

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

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

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

(3) OPSEC and MILDEC are mutually supportive and, as such, should be fully integrated at all levels in order to maximize effective support to friendly operations, activities, plans, and capabilities. MILDEC supports OPSEC by providing potential countermeasure development, approval, and implementation support. OPSEC supports MILDEC by utilizing the OPSEC process to identify risks which can potentially be mitigated by MILDEC.

(a) DISO. A DISO is a MILDEC activity that protects friendly operations, personnel, programs, plans, capabilities, equipment, and other assets against foreign intelligence entity (FIE) collection. The intent of a DISO is to create multiple false indicators to confuse or make friendly force intentions harder to interpret by a FIE and other intelligence gathering apparatus, limiting the ability of a FIE to collect accurate intelligence on friendly forces. Unlike MILDEC, DISO is general in nature; it is not specifically targeted against particular adversary decision makers, but instead is used to protect friendly operations and forces by obfuscating friendly capabilities, intent, or vulnerabilities.

(b) OPSEC planners and program managers have a supporting relationship to MILDEC planners regarding the development, approval, and implementation of DISO activities. **OPSEC planners are not authorized to conduct MILDEC operations.** DISO activities are planned or executed in coordination with the command MILDEC officer.

For further guidance on MILDEC, refer to JP 3-13-4, Military Deception.

5. Operations Security Process in Planning

a. **OPSEC Planning.** OPSEC planning is accomplished by applying the process from Chapter II, "The Operations Security Process," to a specific plan, operation, or activity. While the OPSEC program is broad and far reaching, OPSEC planning's focus is narrow in scope to support the commander's intent.

b. **Identify Critical Information.** The OPSEC planner identifies the critical information specific to the plan, operation, or activity and ensures it is promulgated to all planners. The critical information may change through phases of the operation and must be updated.

c. **Analyze Threat.** The planner evaluates the potential adversaries that have both intent and capability to exploit the critical information in regards to the plan, operation, or activity. Threat analyzed for the OPSEC program will be different based on locations and purpose of the operation or activity, which will require reevaluating the adversary's intent.

d. **Analyze Vulnerabilities.** Planning or conducting operations and activities will increase the likelihood of indicators and create vulnerabilities for exploitation. The

OPSEC planner looks at each COA of the plan, operation, or activity from an adversarial perspective to determine where the command is vulnerable.

e. **Assess Risk.** For each vulnerability identified, the planner assesses the adversary's probability of collection and the impact if they are successful. The risk is then applied to the COA analysis to determine which COA is supportable from an OPSEC perspective or for its impact to the operation or activity. Countermeasures are then recommended to mitigate the vulnerability.

f. **Apply Countermeasures.** Once countermeasures are selected, the planner assigns responsibilities to complete the actions and develop an assessment plan to determine their effectiveness.

See Chairman of the Joint Chiefs of Staff Manual (CJCSM) 3130.03, Adaptive Planning and Execution (APEX) Planning Formats and Guidance, *for a sample OPSEC plan.*

6. Planning Coordination

a. **General.** OPSEC coordination is continuous across all phases of an operation and from the strategic to tactical levels of operations. OPSEC planning is integrated with post-conflict activities, which may be transitioned to a foreign military or government, nongovernmental organizations (NGOs), or intergovernmental organization (IGO) 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. All JPG members should have OPSEC training.

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

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

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

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

7. Joint and Interagency Planning

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

b. **Joint Interagency Coordination Group (JIACG).** When formed at a CCMD, the JIACG provides a venue to integrate other USG departments and agencies into joint operation planning. The IO cell within the joint staff coordinates OPSEC planning efforts with the JIACG throughout the joint operation planning process.

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

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

8. Multinational Planning

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

b. Multinational operations and activities require close cooperation among all forces and can serve to mass strengths, reduce vulnerabilities, and provide legitimacy. OPSEC countermeasures that apply to joint operations are also appropriate for multinational situations. Planners must consider some PNs may have little to no OPSEC capability and rely on nonsecure communications, such as free E-mail accounts and social networking sites, for the conduct of routine operations. Commanders at all levels need to balance the need to share information with PNs with the realization that once shared, the information may be available for collection. Military planners need to ensure all of these

relationships are included in developing the CIL, identifying OPSEC indicators, and applying OPSEC countermeasures.

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

d. Intelligence. The collection, production, and dissemination of intelligence can be a major challenge. Multinational force members normally operate separate intelligence systems in support of their own policy and military forces. JFCs should establish a system that optimizes each nation's contributions and provides member forces a common intelligence picture, tailored to their requirements and consistent with disclosure policies of member nations.

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

(2) The National Disclosure Policy implements National Security Decision Memorandum 119, *Disclosure of Classified United States Military Information to Foreign Governments and International Organizations,* which establishes US policy governing the disclosure of classified military information to foreign governments. It promulgates national policy and procedures in the form of specific disclosure criteria and limitations, definitions of terms, release arrangements, and other guidance. It also establishes interagency mechanisms and procedures for the effective implementation of the policy. In the absence of sufficient guidance, JFCs should share only information that is mission-essential, affects lower-level operations, facilitates combat identification, and is perishable.

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

9. Intergovernmental and Nongovernmental Organization Considerations

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

(1) **IGOs** are organizations created by a formal agreement (e.g., a treaty) between two or more governments and may be established on a global, regional, or

functional basis for wide-ranging or narrowly-defined purposes. They are formed to protect and promote national interests shared by member states.

(2) **NGOs** are private, self-governing, not-for-profit organizations dedicated to alleviating human suffering; promoting education, health care, economic development, environmental protection, human rights, and conflict resolution; or encouraging the establishment of democratic institutions and civil society.

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

c. **Integration.** It is vital to integrate any and all willing mission partners, which may include IGOs and NGOs, interagency, and military partners operating in the operational area into joint operation planning as early as possible so an integrated comprehensive and achievable OPSEC plan can be developed. Initial requirements for integration include clarification of objectives, understanding how partners intend to conduct activities, establishment of liaison and deconfliction procedures, and identification of vulnerabilities and possible countermeasures to adversary exploitation. Whether planning is based on APEX through the joint operation planning process or on established foreign or alliance planning processes, planners should work to recognize and understand the differing institutional cultural values, interests and concerns, moral and ethical values, rules of engagement, and legal constraints and allow for complications in planning and execution in multiple languages.

For additional information on interorganizational coordination, see JP 3-08, Interorganizational Coordination During Joint Operations.

THE "BLACK HOLE": OPSEC DURING PLANNING

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

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

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

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

Intentionally Blank

CHAPTER IV
OPERATIONS SECURITY ASSESSMENTS AND SURVEYS

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

George Washington
1st President of the United States (1789-1797)

1. Assessments and Surveys

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

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

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

c. **Uniqueness**

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

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

(3) During noncombat operations, to include military engagement, security cooperation, and deterrence, assessments generally seek to correct weaknesses that disclose information useful to potential adversaries in the event of future conflict. Many activities, such as operational unit tests, drills, practice alerts, and major exercises, are of great interest to a potential adversary because they provide insight into friendly readiness, plans, crisis procedures, and C2 capabilities that enhance that adversary's planning.

d. **OPSEC Assessments Versus Security Inspections**

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

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

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

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

(5) To obtain accurate information, an assessment team should try to create an environment that promotes positive cooperation and assistance from the organizations participating in the operation or activity being assessed. If team members must question individuals, observe activities, and otherwise gather data during the course of the assessment, then they should make it clear they are not inspectors and their objectives are nonpunitive.

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

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

e. **Assessments and Surveys**

(1) **OPSEC Assessment.** OPSEC assessments should be conducted as needed in order to establish a baseline signature for the respective units when conditions or mission profile dictate, and to identify any changes in "signatures" based on an operation, activity, exercise, or support function to determine the likelihood that critical information

can be protected from the adversary's intelligence collection systems. An OPSEC assessment is normally run by the OPSEC program manager and performed by the unit's OPSEC working group. An assessment may be conducted with a small team of individuals from within an organization with or without assistance from subject matter experts. The scope of an OPSEC assessment is usually limited to events and/or activities within that organization.

(2) **OPSEC Survey.** Also known as an external assessment, threat-based comprehensive OPSEC surveys are conducted, at a minimum, every three years. A survey usually requires a team of external subject matter experts from multiple disciplines to simulate adversary intelligence processes. An OPSEC survey should focus on the organization's ability to adequately protect critical information from adversary intelligence exploitation during planning, preparation, execution, and post-execution phases of any operation or program. These surveys may include telecommunications monitoring, radio frequency monitoring, network and computer systems assessment, and open-source collection. Survey teams should use collection techniques of known adversaries. In accordance with DODD 5205.02E, *DOD Operations Security (OPSEC) Program*, an OPSEC survey is required every three years. See Figure IV-1 for an assessment–survey comparison.

(3) **COMSEC Monitoring Assessment.** JCMA and other Service organizations conduct operations vital to identifying OPSEC disclosures by monitoring, collecting, analyzing, and reporting on sensitive information released from DOD encrypted and unencrypted telecommunications signals and automated information systems such as computer networks, telephones, E-mail, and websites. Their purpose is to identify vulnerabilities exploitable by potential adversaries and to recommend countermeasures and corrective actions. These assessments are often limited in scope and duration, but can be designed to monitor communications persistently up to the enterprise level.

(a) Activities that warrant OPSEC surveys include, but are not limited to, research, development, test, and evaluation; acquisitions; theater security cooperation events; port calls; treaty verification; nonproliferation protocols; international agreements; force protection operations; special access programs; and activities that prepare, sustain, or employ Military Services.

(b) DOD components identify and prioritize OPSEC survey requirements and outline procedures for requesting OPSEC survey support from the appropriate organizations.

Assessment–Survey Comparison

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

Figure IV-1. Assessment–Survey Comparison

2. Assessment Planning

a. **Introduction.** An assessment must be thoroughly planned to ensure it assesses the vulnerabilities to loss of critical information. Allot sufficient time in the planning phase for a thorough review of pertinent documentation, for formal and informal coordination and discussions. The following actions will focus the planning phase:

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

c. **Select Team Members.** Assessment team members should be selected for their analytical, observational, and problem-solving abilities. Team members should represent the functional areas of intelligence, CI, security, communications, logistics, plans,

cybersecurity, PA, contracting, acquisition, and administration. When appropriate, specialists from other functional areas, such as transportation or chemical, biological, radiological, and nuclear, will participate.

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

e. **Review Empirical Studies.** Empirical studies, such as COMSEC or CI reports, simulate aspects of the adversary intelligence threat and support vulnerability findings.

3. Assessment Execution

a. **Introduction.** The primary action during an assessment is to collect data. Data is collected through observation of activities, document collection, and personnel interviews. Data may also be acquired through concurrent ongoing empirical data collection, such as COMSEC monitoring.

b. **Team Members.** 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.

c. **Findings.** 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.

4. Analysis and Reporting

a. **Introduction.** To complete the assessment, the OPSEC team must correlate the data to identify previously identified 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. **Reporting.** Once complete, the analysis should be captured in a report to provide the command the information and to serve as an archival tool for future assessments.

For further information, see DOD 5205.02-M, DOD Operations Security (OPSEC) Program Manual.

Intentionally Blank

APPENDIX A
OPERATIONS SECURITY INDICATORS

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

1. Indicators of General Military Force Capabilities

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

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

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

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

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

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

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

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

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

j. Personnel training in protective equipment or practicing decontamination.

2. Indicators of General Command and Control Capabilities

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

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

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

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

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

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

3. General Indicators from Communications Usage

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

b. Establishing new communications networks. 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 networks could prompt them to implement additional intelligence collection to discern friendly activity more accurately.

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

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

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

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

g. Using social media either personally or through the command, broadcasting movements, capabilities, locations, personnel, etc.; including information gleaned from family member social media.

4. Sources of Possible Indicators for Equipment and System Capabilities

a. Unencrypted emissions during tests and exercises.

b. Public media, particularly technical journals.

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

d. The equipment or system hardware itself.

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

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

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

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

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

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

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

5. Indicators of Preparations for Operations or Activities

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

a. Provisioning of special supplies for participating elements.

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

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

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

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

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

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

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

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

j. Providing increased or tailored personnel training.

k. Holding rehearsals to test concepts of operation.

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

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

n. Arranging for tugs and pilots.

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

p. Declaring unusual off-limits restrictions.

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

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

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

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

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

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

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

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

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

z. New or increased contracting activity.

6. Sources of Indicators During the Execution Phase

a. Unit and equipment departures from normal bases.

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

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

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

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

f. Alert of civilians in operational areas.

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

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

i. Changes in oceanographic high frequency facsimile transmissions.

j. Changes in the activity over the DOD information network.

7. Indicators of Post-Engagement Residual Capabilities

a. Repair and maintenance facilities' schedules.

b. Urgent calls for maintenance personnel.

c. Movement of supporting resources.

d. Medical activity.

e. Unusual resupply and provisioning of an activity.

f. Assignment of new units from other areas.

g. Search and rescue activity.

h. Personnel orders.

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

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

APPENDIX B
FUNCTIONAL OUTLINES AND PROFILES

1. Intelligence Collection Operations

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

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

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

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

e. **Examples of Typical Indicators**

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

(2) Increased traffic on intelligence communications networks.

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

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

(5) Increased activity of friendly agent networks.

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

(7) Alterations in the orbits of intelligence satellites.

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

(9) Requests for maps and other topographic material.

(10) Appearance of OPSEC assessment team.

2. Logistics

a. **General.** The completed logistic profile presents a picture of logistic activities conducted in preparation for an impending operation. As in the administration function,

the long lead time for some preparations gives early warning of forthcoming operations if events are compromised.

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

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

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

e. **Examples of Typical Indicators**

(1) Special equipment issue.

(2) Pre-positioning of equipment and supplies.

(3) Increased weapons and vehicle maintenance.

(4) Petroleum, oils, and lubricants stockpiling.

(5) Upgrading lines of communications.

(6) Ammunition stockpiling.

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

(8) Arrival of new logistic units and personnel.

(9) Increased requisition of supplies.

(10) Increased traffic on logistic communications networks.

(11) Changes in normal delivery patterns.

(12) Appearance of OPSEC assessment team.

3. Communications

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

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

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

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

e. **Examples of Typical Indicators**

(1) Increased radio and telephone traffic.

(2) Increased communications checks.

(3) Appearance of new stations in network.

(4) New frequency and call-sign assignments.

(5) New codes and authenticators.

(6) Radio silence.

(7) Changing call-up patterns.

(8) Use of maintenance frequencies to test equipment.

(9) Communications command post exercises.

(10) Appearance of different cryptographic equipment and materials.

(11) Unclassified network activity.

(12) Appearance of OPSEC assessment team.

4. Operations

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

b. **Planned Event Sequence.** OPLAN, OPORD, standard operating procedure (SOP).

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

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

e. **Examples of Typical Indicators**

(1) Rehearsals and drills.

(2) Special tactics refresher training.

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

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

(5) Artillery registration in new objective area.

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

(7) Appearance of new attached units.

(8) Issuance of new equipment.

(9) Changes in major unit leadership.

(10) Repositioning of maneuver units.

(11) Appearance of OPSEC assessment team.

5. Administration and Support

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

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

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

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

e. **Examples of Typical Indicators**

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

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

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

(4) Changes to mailing addresses.

(5) New unit designators on mail.

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

(7) Medical supply stockpiling.

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

(9) Appearance of OPSEC assessment team.

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

APPENDIX C
SAMPLE OPERATIONS SECURITY PLAN

OPLAN/OPORD: Tab C (Operations Security) to Appendix 3 (Information Operations) to Annex C (Operations). See the current CJCSM 3130.03, *Adaptive Planning and Execution (APEX) Planning Formats and Guidance,* for the current format.

References: List documents essential to this annex.

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

a. ( ) **Enemy Forces**

(1) ( ) **Current Intelligence Assessment.** Identify the likely adversaries and their respective goals. Identify the adversary's assessment of friendly operations, capabilities, and intentions. Identify the adversary's knowledge of critical information related to the friendly operation addressed in the base plan. State the estimated enemy's assessment of friendly operations, capabilities, and intentions. Specifically, address any known enemy knowledge of the friendly operations covered in the basic plan.

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

b. ( ) **Friendly**

(1) ( ) **Friendly Operations.** Describe the major actions to be conducted by friendly forces in executing the base plan.

(2) ( ) **Critical Information.** Identify specific facts about friendly intentions, capabilities, and activities vitally needed by an adversary to guarantee failure or unacceptable consequences for friendly mission accomplishment. Include the critical information of higher headquarters and list the critical information by phase. List the

identified critical information. In phased operations, list it by phase; information that is critical in an early phase may not require protection in later phases.

c. ( ) **Assumptions.** Identify any assumptions upon which this OPSEC plan is based. Identify any assumptions unique to OPSEC planning.

2. ( ) **Mission.** Refer to base plan.

3. ( ) **Execution**

a. ( ) **Concept of Operations.** Discuss the role of OPSEC in the commander's CONOPS. Describe the general concept for the implementation of planned OPSEC measures. Describe by phase and major activity (maneuver, logistics, communications, etc.), if appropriate. Address OPSEC support to other IRCs and activities. Continually assess the unclassified, but sensitive, information vital to the base plan.

b. ( ) **Tasks.** Identify specific OPSEC measures to be executed by phase, if appropriate. Assign responsibility for execution to appropriate subordinate elements and support commands or agencies. Particularly detailed or lengthy listings should be added as an exhibit to the OPSEC tab.

c. ( ) **Coordinating Instructions.** Identify any requirements for the coordination of OPSEC measures between subordinate elements and support commands or agencies. Address required coordination with PA. Provide guidance on termination of OPSEC measures. Address the declassification and public release of the OPSEC plan to prevent adversaries from developing countermeasures to successful OPSEC measures. Describe OPSEC assessments or surveys conducted in support of this plan.

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

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

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

4. ( ) **Administration and Logistics.** Identify any OPSEC-related administrative or logistics support requirements in this section. List OPSEC measures protecting administrative or logistics activities in the execution paragraph 3.

5. ( ) **Command and Control**

a. ( ) **Command Relationships**

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

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

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

b. ( ) **Command, Control, Communications, and Computer Systems.** Address any special or unusual OPSEC-related command, control, communications, and computer system requirements. List OPSEC measures protecting command, control, communications, and computer system activities in the execution paragraph 3.

Intentionally Blank

APPENDIX D
REFERENCES

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

1. General Publications

a. *National Disclosure Policy*.

b. National Security Decision Memorandum 119, *Disclosure of Classified United States Military Information to Foreign Governments and International Organizations.*

c. National Security Decision Directive 298, *National Operations Security Program*.

2. Department of Defense Publications

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

b. DODD 5205.02E, *DOD Operations Security (OPSEC) Program.*

c. DODD S-5205.61, (U) *DOD Cover and Cover Support Activities.*

d. DOD Instruction S-3604.01, *Department of Defense Military Deception (MILDEC).*

e. DOD Manual 5200.01, Volume 4, *DOD Information Security Program: Controlled Unclassified Information (CUI)*.

3. Chairman of the Joint Chiefs of Staff Publications

a. CJCSI 3211.01F, *(U) Joint Policy for Military Deception.*

b. CJCSI 3213.01D, *Joint Operations Security.*

c. CJCSI 3320.01D, *Joint Electromagnetic Spectrum Operations (JEMSO).*

d. CJCSI 5120.02D, *Joint Doctrine Development System.*

e. CJCSI 5714.01D, *Policy for the Release of Joint Information.*

f. CJCSM 3122.01A, *Joint Operation Planning and Execution System (JOPES), Volume I (Planning Policies and Procedures).*

g. CJCSM 3130.03, *Adaptive Planning and Execution (APEX) Planning Formats and Guidance.*

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

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

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

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

l. JP 3-08, *Interorganizational Coordination During Joint Operations*.

m. JP 3-09, *Joint Fire Support*.

n. JP 3-11, *Operations in Chemical, Biological, Radiological, and Nuclear Environments.*

o. JP 3-12, *Cyberspace Operations*.

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

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

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

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

t. JP 3-60, *Joint Targeting.*

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

v. JP 5-0, *Joint Planning.*

APPENDIX E
ADMINISTRATIVE INSTRUCTIONS

1. User Comments

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

2. Authorship

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

3. Supersession

This publication supersedes JP 3-13.3, *Operations Security*, 4 January 2012.

4. Change Recommendations

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

TO: JOINT STAFF WASHINGTON DC//J35//JFC

b. Routine changes should be submitted electronically to the Deputy Director, Joint Education and Doctrine, ATTN: Joint Doctrine Analysis Division, 116 Lake View Parkway, Suffolk, VA 23435-2697, and info the lead agent and the Director for Joint Force Development, J-7/JED.

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

5. Distribution of Publications

Local reproduction is authorized, and access to unclassified publications is unrestricted. However, access to and reproduction authorization for classified JPs must be IAW DOD Manual 5200.01, Volume 1, *DOD Information Security Program: Overview, Classification, and Declassification*, and DOD Manual 5200.01, Volume 3, *DOD Information Security Program: Protection of Classified Information.*

6. Distribution of Electronic Publications

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

b. Only approved JPs are releasable outside the combatant commands, Services, and Joint Staff. Defense attachés may request classified JPs by sending written requests to Defense Intelligence Agency (DIA)/IE-3, 200 MacDill Blvd., Joint Base Anacostia-Bolling, Washington, DC 20340-5100.

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

GLOSSARY

PART I—ABBREVIATIONS AND ACRONYMS

APEX	Adaptive Planning and Execution
C2	command and control
CCDR	combatant commander
CCMD	combatant command
CI	counterintelligence
CIL	critical information list
CJCS	Chairman of the Joint Chiefs of Staff
CJCSI	Chairman of the Joint Chiefs of Staff instruction
CJCSM	Chairman of the Joint Chiefs of Staff manual
CMOC	civil-military operations center
COA	course of action
COMSEC	communications security
CUI	controlled unclassified information
DIA	Defense Intelligence Agency
DISO	deception in support of operations security
DOD	Department of Defense
DODD	Department of Defense directive
EA	electronic attack
E-mail	electronic mail
FIE	foreign intelligence entity
IGO	intergovernmental organization
IO	information operations
IOSS	Interagency Operations Security Support Staff
IRC	information-related capability
JCMA	joint communications security monitoring activity
JCMOTF	joint civil-military operations task force
JFC	joint force commander
JIACG	joint interagency coordination group
JIPOE	joint intelligence preparation of the operational environment
JOSE	Joint Operations Security Support Element (Joint Staff)
JP	joint publication
JPG	joint planning group
MILDEC	military deception
MOE	measure of effectiveness
MOP	measure of performance

NGO	nongovernmental organization
NSA	National Security Agency
OEG	operations security executive group
OPLAN	operation plan
OPORD	operation order
OPSEC	operations security
PA	public affairs
PAO	public affairs officer
PN	partner nation
SIGINT	signals intelligence
SOP	standard operating procedure
USG	United States Government

PART II—TERMS AND DEFINITIONS

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

indicator. 1. In intelligence usage, an item of information which reflects the intention or capability of an adversary to adopt or reject a course of action. (JP 2-0) 2. In operations security usage, data derived from friendly detectable actions and open-source information that an adversary can interpret and piece together to reach conclusions or estimates of friendly intentions, capabilities, or activities. (JP 3-13.3) (Approved for incorporation into JP 1-02.)

operations security. A capability that identifies and controls critical information, indicators of friendly force actions attendant to military operations, and incorporates countermeasures to reduce the risk of an adversary exploiting vulnerabilities. Also called **OPSEC.** (Approved for incorporation into JP 1-02.)

operations security assessment. An evaluative process to determine the likelihood that critical information can be protected from the adversary's intelligence. (Approved for incorporation into JP 1-02.)

operations security countermeasures. Methods and means to gain and maintain essential secrecy about critical information. (JP 1-02. SOURCE: JP 3-13.3)

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

operations security planning guidance. Guidance that defines the critical information requiring protection from the adversary and outlines provisional measures to ensure secrecy. (JP 1-02. SOURCE: JP 3-13.3)

operations security survey. A collection effort by a team of subject matter experts to reproduce the intelligence image projected by a specific operation or function simulating hostile intelligence processes. (JP 1-02. SOURCE: JP 3-13.3)

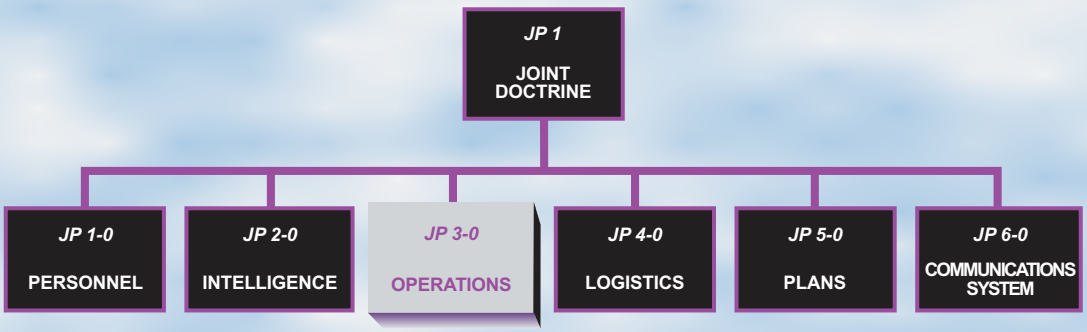
operations security vulnerability. A condition in which friendly actions provide operations security indicators that may be obtained and accurately evaluated by an adversary in time to provide a basis for effective adversary decision making. (JP 1-02. SOURCE: JP 3-13.3)

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

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

Intentionally Blank

JOINT DOCTRINE PUBLICATIONS HIERARCHY



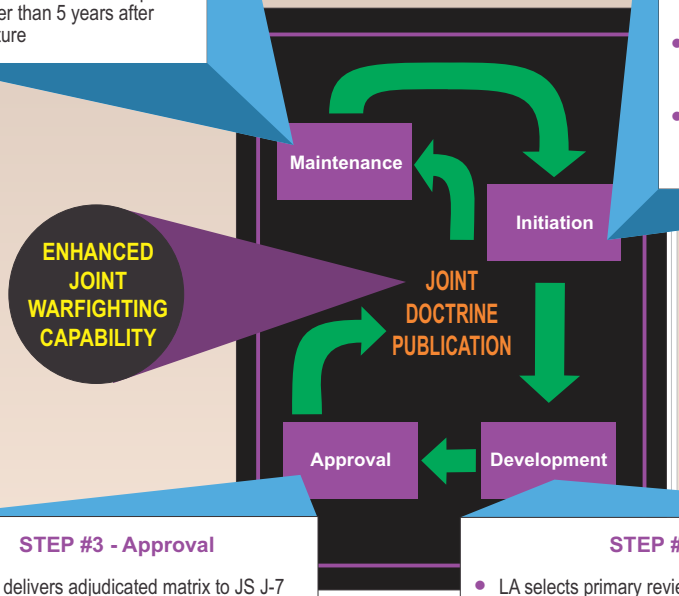
All joint publications are organized into a comprehensive hierarchy as shown in the chart above. **Joint Publication (JP) 3-13.3** is in the **Operations** series of joint doctrine publications. The diagram below illustrates an overview of the development process:

STEP #4 - Maintenance

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

STEP #1 - Initiation

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



STEP #3 - Approval

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

STEP #2 - Development

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


JOINT
CHIEFS OF STAFF