ATP 3-13.3

ARMY OPERATIONS SECURITY FOR DIVISION AND BELOW

JULY 2019

DISTRIBUTION RESTRICTION: Approved for public release; distribution is unlimited.

Headquarters, Department of the Army

Army Techniques Publication
No. 3-13.3

Headquarters
Department of the Army
Washington, DC, 16 July 2019

Army Operations Security for Division and Below

Contents

Figures

DISTRIBUTION RESTRICTION: Approved for public release; distribution is unlimite**d**

Tables

Preface

ATP 3-13.3, Army Operations Security for Division and below, provides doctrinal guidance on how to identify, control, and protect essential elements of friendly information during combat operations for tactical units at echelons division and below.

The principal audience for ATP 3-13.3 is all members of the profession of arms; however, the primary users of this publication are tactical unit commanders, operations security planners, and staffs. Commanders and staffs of U.S. Army headquarters serving as a joint task force or multinational headquarters should also refer to applicable joint or multinational doctrine concerning the range of military operations and joint or multinational forces. Trainers and educators throughout the Army will also use this publication.

Commanders, staffs, and subordinates ensure their decisions and actions comply with applicable United States, international, and, in some cases, host-nation laws and regulations. Commanders at all levels ensure their Soldiers operate in accordance with the law of war and the rules of engagement (see FM 27-10).

ATP 3-13.3 uses joint terms where applicable. Selected joint and Army terms and definitions appear in both the glossary and the text. For definitions shown in the text, the term is italicized and the number of the proponent publication follows the definition. This publication is not the proponent for any Army terms.

Operating forces use the doctrinal term essential elements of friendly information. The corresponding term in joint doctrine is critical information. The Army and joint definitions describe identical processes with the same objective: to protect information that can impede or prevent the force from accomplishing its mission. For the purpose of this document, the two terms are interchangeable. While in support of joint operations, operations security planners will use the joint term critical information, as appropriate. Operations security planners supporting Army operations will use the Army term essential elements of friendly information, in agreement with ADP 5-0, ADRP 5-0, and Army planning methodologies.

ATP 3-13.3 applies to the Active Army, Army National Guard, Army National Guard of the United States, and the United States Army Reserve, unless otherwise stated.

The proponent for this publication is the United States Army Combined Arms Center, Information Operations Proponent Office. The preparing agency is the Combined Arms Doctrine Directorate, United States Army Combined Arms Center. Send written comments and recommendations on a DA Form 2028 (*Recommended Changes to Publications and Blank Forms*) directly to the Commander, United States Army Combined Arms Center and Fort Leavenworth, ATTN: ATZL-MCK-D (ATP 3-13.3), 300 McPherson Avenue, Fort Leavenworth, KS 66027-2337; by email to: usarmy.leavenworth.mccoe.mbx.cadd-org-mailbox@mail.mil; or submit an electronic DA Form 2028.

This page intentionally left blank.

Introduction

The purpose of this ATP is to provide a doctrinal operations security reference for Army tactical unit commanders, operations security planners, staffs, and unit trainers at division and below. Other doctrinal references useful to a more complete understanding of operations security include ADRP 5-0, ADRP 6-0, ADP 3-37, FM 6-0, and JP 3-13.3.

The Army operations security process is a systematic method used to identify, control, and protect essential elements of friendly information. An essential element of friendly information is a critical aspect of a friendly operation that, if known by the enemy, would subsequently compromise, lead to failure, or limit success of the operation and therefore should be protected from enemy detection. Traditional security programs protect classified information, but are not necessarily designed to protect essential elements of friendly information. Properly implemented operations security works in coordination with traditional security programs to protect essential elements of friendly information.

The Army Protection Program, a management framework to synchronize, prioritize, and coordinate protection policies and resources, highlights operations security as an additional protection task that commanders and staffs must synchronize and integrate, along with other capabilities and resources, to preserve combat power. Commanders designate a member of the staff to serve as the unit's operations security planner. The operations security planner—typically a standing member of the unit's protection working group that brings together representatives of all staff elements concerned with protection— ensures that operations security is considered during the military decisionmaking process and incorporated within the unit's scheme of protection.

The operations security planner analyzes unit's information activities, operational patterns and routines, signatures, and other activities that reveal unit-specific operational information and other associated observables. The operations security planner assesses whether such information or indicators could reasonably be observed by enemy or adversary forces known or suspected of conducting surveillance, reconnaissance, or intelligence collection activities directed against the unit. After identifying potentially vulnerable essential elements of friendly information, the operations security planner recommends them to the commander, along with a variety of measures to prevent their compromise.

Commanders direct measures and countermeasures to reduce enemy observation and exploitation of friendly actions. These measures include concentrating forces and hiding friendly movements and rehearsals. Additionally, Army divisions and echelons below employ countermeasures such as camouflage, concealment, and decoys as an integral part of unit standard operating procedures.

ATP 3-13.3 contains four chapters and one appendix. A brief description of each follows:

Chapter 1 discusses the fundamentals of operations security, provides a list of operations security-related terms, and describes commander and operations security planner responsibilities.

Chapter 2 describes the operations security process in detail, discusses how the process should be incorporated into operations and planning, identifies each step of the process, suggests several items to consider for operations security guidance, and provides an example of an operations security estimate.

Chapter 3 examines an operations security planner's role in each step of the military decisionmaking process.

Chapter 4 looks at the tools available to monitor, evaluate, and refine unit measures and countermeasures.

Appendix A offers tips and recommendations for developing the operations security appendix of an operational order and provides an example of a completed operations security appendix.

This page intentionally left blank.

Chapter 1

Overview of Operations Security at Division and Below

1-1. Properly implemented measures and countermeasures can protect essential elements of friendly information from enemy or adversary observation and collection. Compromised essential elements of friendly information bolster enemy or adversary efforts to exploit Army units. These compromises can lead to the design and development of enemy or adversary systems, tactics, training, and make force preparations capable of countering Army unit capabilities, activities, and intentions. Preventive measures recommended by an operations security (OPSEC) planner lessen and mitigate exploitation of known or suspected unit limitations and vulnerabilities.

1-2. Access to essential elements of friendly information often occurs because of day-to-day activities that, to the casual observer, seem commonplace. For example, bits of information conveyed through communications such as unsecure radio transmissions or unsecure telephone calls, unencrypted email messages containing sensitive information, public releases or briefings, or friendly conversations in public areas permit our enemies and adversaries to piece together an Army unit's capabilities, activities, limitations, and intentions. Proper observance of preventive measures keeps essential elements of friendly information from appearing in open sources and from falling into the hands of our enemies and adversaries.

FUNDAMENTALS OF OPERATIONS SECURITY

1-3. Army security programs focus on classified information, but OPSEC focuses on protecting unclassified information, which includes denying essential elements of friendly information to our enemies and adversaries. OPSEC's overarching goal is to eliminate, reduce, or conceal unclassified indicators that could compromise both classified information as well as essential elements of friendly information about an Army unit. OPSEC and security programs work cooperatively but separately to achieve this goal. Because the OPSEC planner and security manager are separate positions with distinct goals, they should be filled by different people.

1-4. Understanding the terms most often used by OPSEC planners greatly enhances understanding of OPSEC fundamentals. These terms are—

- *Controlled unclassified information* is unclassified information to which access or distribution limitations have been applied according to national laws, policies, and regulations of the U.S. Government. It includes U.S. information that is determined to be exempt from public disclosure according to DODD 5230.25, DODD 5400.07, AR 25–55, AR 530–1, and so on, or that is subject to export controls according to the International Traffic in Arms Regulations or the Export Administration Regulations (AR 530-1).
- *Countermeasures* are that form of military science that, by the employment of devices and/or techniques, has as its objective the impairment of the operational effectiveness of enemy activity (JP 3-13.1). They can be deployed preemptively or reactively.
- An *essential element of friendly information* is a critical aspect of a friendly operation that, if known by the enemy, would subsequently compromise, lead to failure, or limit success of the operation and therefore should be protected from enemy detection (ADRP 5-0).
- An *indicator* is, in OPSEC 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).
- *Operations security* 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 (JP 3-13.3).

- *Operations security assessment* is an evaluative process to determine the likelihood that critical information can be protected from the adversary's intelligence (JP 3-13.3).
- *Operations security compromise* is the disclosure of critical information or sensitive information which has been identified by the command and any higher headquarters that jeopardizes the unit's ability to execute its mission or to adequately protect its personnel and/or equipment (AR 530-1).
- An *operations security survey* is 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 3-13.3).
- *Operations security vulnerability* is a condition in which friendly actions provide operations security indicators that may be obtained and accurately evaluated by an adversary in time to provide a basis for effective adversary decision making (JP 3-13.3).
- *Sensitive* is an agency, installation, person, position, document, material, or activity requiring special protection from disclosure that could cause embarrassment, compromise, or threat to the security of the sponsoring power (JP 2-01).

1-5. Effective and disciplined OPSEC is employed during all decisive actions. Units routinely employ OPSEC to protect essential elements of friendly information. This helps to prevent enemy or adversary reconnaissance and other information collection capabilities from gaining an advantage because the threat has knowledge of identifiable or observable unit-specific information or activities. OPSEC contributes to the unit's offensive operations by enabling efforts that slow the adversary decision cycle and affect the quality of the enemy commander's decisions. OPSEC supports the unit's defensive operations by denying the enemy information that could be used for targeting or attacking the unit. OPSEC is especially key during retrograde operations, where preventing and limiting an enemy or adversary's ability to discern unit capabilities, activities, limitations, and intentions is paramount. The retrograde is a defensive task that involves organized movement away from the enemy (see ADP 3-90 and FM 3-90-1 for more on retrograde movement and retrograde operations).

FORCE PROTECTION

1-6. *Force protection* is preventive measures taken to mitigate hostile actions against Department of Defense personnel (to include family members), resources, facilities, and critical information. Also called FP (JP 3-0). Measures and countermeasures support force protection actions to negate enemy and adversary access and the subsequent collection of information needed to plan and carry out actions against the unit. The unit OPSEC planner recommends and implements measures, countermeasures, and traditional security measures to identify and protect essential elements of friendly information.

DECEPTION

1-7. OPSEC, integrated and synchronized in combination with other protection measures, may be employed with deception to ensure that only desired events reach the enemy and supported operations are concealed. False indicators are wrapped in significant amounts of factual information to enhance their acceptance but not compromise the supported operation. Without OPSEC, the enemy might not believe the deception suggested by the false indicators. This is especially important where observable indicators may be present and collectable by the enemy that counter the deception story and inadvertently reveal true unit preparations in support of a planned or ongoing operation. At times, unit commanders employ deception in support of OPSEC to create multiple false indicators that confuse enemy or adversary forces operating in the unit's area of operations, making unit intentions harder to interpret. A deception in support of OPSEC uses controlled information about friendly force capabilities, activities, and intentions to shape perceptions. It targets and counters intelligence, surveillance, and reconnaissance capabilities to distract intelligence collection away from, or provide cover for, unit operations. A deception in support of OPSEC is a relatively easy countermeasure to use and is appropriate for use at battalion-level and below. To be successful, OPSEC and deception requirements must achieve balance.

REHEARSALS

1-8. Rehearsals of unit operations elevate the opportunity to incur OPSEC risks. Unit commanders must consider that the placement of forces and capabilities, together with large-scale movements of the force, can attract enemy attention and interest. Key personnel rehearsals are less likely to present OPSEC risks than a full dress rehearsal because they generally involve fewer participants and less movement of forces. The terrain model rehearsal is the most popular rehearsal method. It takes less time and fewer resources than a full dress or reduced force rehearsal. An accurately constructed terrain model helps subordinate leaders visualize the commander's intent and concept of operations. When possible, commanders place the terrain model where it overlooks the actual terrain of the area of operations. This rehearsal can present OPSEC risks if the area around the rehearsal site is unsecured or open to unintended or unwanted observation, as assembled commanders and their vehicles can draw enemy attention. When employing rehearsals as a prelude to operations, unit commanders and planners must ensure the site is secure from enemy intelligence, surveillance, and reconnaissance activities, and also must sanitize materials and information used to construct the terrain model after completing the rehearsal. The OPSEC risk is further exacerbated if these materials are uploaded to the unit information network, where they can become the subject of enemy cyber exploitation.

1-9. Two techniques to reduce OPSEC risk are to use either a sketch map in place of the terrain model, or a map rehearsal. Procedures for using a sketch map are identical to a terrain-model rehearsal and can be used almost anywhere, day or night. After use, units must sanitize, secure, or destroy the sketch map. A map rehearsal relies on the use of a map with a combined information overlay of the same scale used to plan the operation. Close control of the map and overlays reduces the opportunity for OPSEC compromises. Commanders, having consulted their OPSEC planner, develop a plan to protect the rehearsal from enemy information collection. Sometimes commanders develop an alternate plan that subordinates rehearse, which confuses the enemy without compromising the actual plan. Commanders must be careful, however, to do this without confusing subordinates.

1-10. Commanders and staffs who conduct network rehearsals over wide-area networks or local area networks practice these rehearsals by talking through critical portions of the operation over communications networks in a sequence the commander establishes. If a unit executes a network rehearsal from current unit locations, the OPSEC risk may increase. The enemy might monitor the increased volume of transmissions, potentially resulting in compromised information. To avoid compromise, units employ different communications connectivity from that planned for the operation.

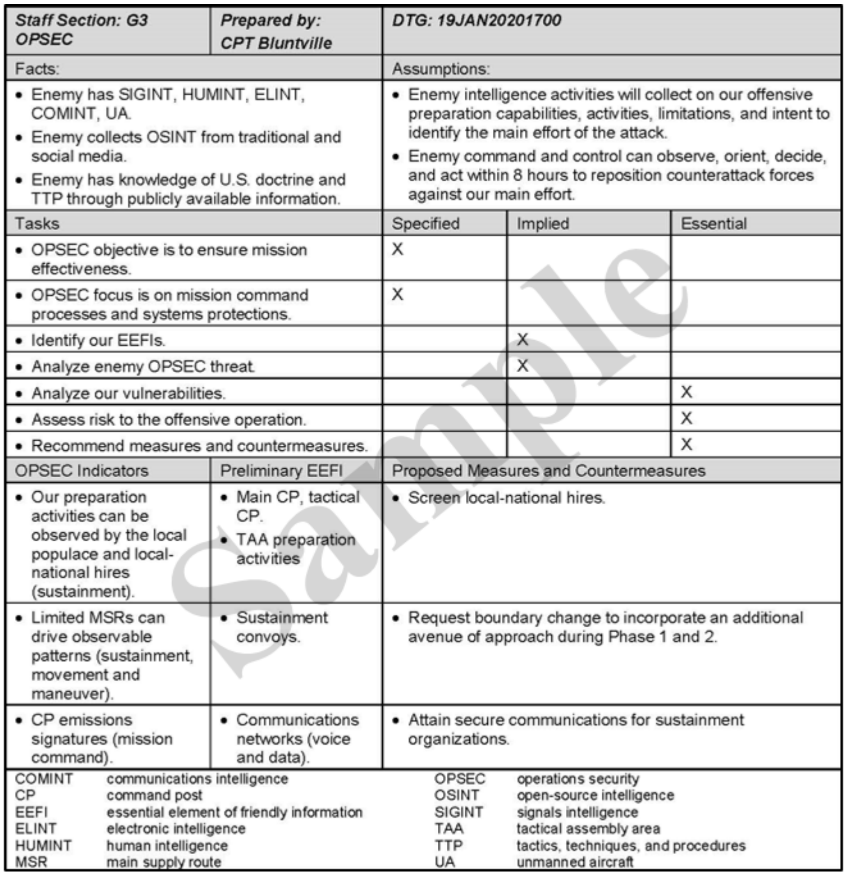
KEY PERSONNEL PROTECTION

1-11. Some key personnel may be designated as high risk. *High-risk personnel* are personnel who, by their grade, assignment, symbolic value, or relative isolation, are likely to be attractive or accessible terrorist targets (JP 3-07.2). Senior commanders and key personnel are at a significantly greater risk during conflicts and peacekeeping operations. These personnel are subject to increased likelihood of physical attacks or kidnapping for political purposes. Information on these key individuals, including their official purpose, travel, and locations in an operational environment, are considered essential elements of friendly information and require the utmost security. Though OPSEC is an operations function and not a security function, both functions work together to ensure OPSEC is integrated into all planning involving key personnel. As stated in paragraph 1-6, the unit OPSEC planner recommends and implements measures in combination with countermeasures and traditional security measures to identify and protect essential elements of friendly information that must not be allowed to appear in the public domain. See FM 3-39 and DOD Instruction O-2000.22 for more information on established policy, responsibilities, and prescribed procedures for designating and protecting DOD high-risk personnel.

OPERATIONS SECURITY RESPONSIBILITIES AT DIVISION AND BELOW

1-12. Army unit commanders, supported by their staff OPSEC planner and primary staff and in accordance with unit standard operating procedure (SOP), implement OPSEC as an integral part of the operations synchronization process. In driving the operations process, commanders understand, visualize, describe, direct, lead, and assess operations. See ADRP 5-0 for more information on the operations process.

1-13. *Understand.* Commanders build their understanding of the problem and an operational environment. The OPSEC estimate helps commanders improve their understanding. Included in this estimate are facts and assumptions, tasks (specified, implied, essential), OPSEC Indicators, Preliminary EEFI, and Proposed Measures and Countermeasures. An example of how to lay out this information is shown in figure 1-1.



Staff Section: G3 OPSEC	***Prepared by: CPT Bluntville***	***DTG: 19JAN20201700***		
Facts:		Assumptions:		
• Enemy has SIGINT, HUMINT, ELINT, COMINT, UA. • Enemy collects OSINT from traditional and social media. • Enemy has knowledge of U.S. doctrine and TTP through publicly available information.		• Enemy intelligence activities will collect on our offensive preparation capabilities, activities, limitations, and intent to identify the main effort of the attack. • Enemy command and control can observe, orient, decide, and act within 8 hours to reposition counterattack forces against our main effort.		
Tasks		Specified	Implied	Essential
• OPSEC objective is to ensure mission effectiveness.		X		
• OPSEC focus is on mission command processes and systems protections.		X		
• Identify our EEFIs.			X	
• Analyze enemy OPSEC threat.			X	
• Analyze our vulnerabilities.				X
• Assess risk to the offensive operation.				X
• Recommend measures and countermeasures.				X
OPSEC Indicators	Preliminary EEFI	Proposed Measures and Countermeasures		
• Our preparation activities can be observed by the local populace and local-national hires (sustainment).	• Main CP, tactical CP. • TAA preparation activities	• Screen local-national hires.		
• Limited MSRs can drive observable patterns (sustainment, movement and maneuver).	• Sustainment convoys.	• Request boundary change to incorporate an additional avenue of approach during Phase 1 and 2.		
• CP emissions signatures (mission command).	• Communications networks (voice and data).	• Attain secure communications for sustainment organizations.		

COMINT	communications intelligence
CP	command post
EEFI	essential element of friendly information
ELINT	electronic intelligence
HUMINT	human intelligence
MSR	main supply route
OPSEC	operations security
OSINT	open-source intelligence
SIGINT	signals intelligence
TAA	tactical assembly area
TTP	tactics, techniques, and procedures
UA	unmanned aircraft

Figure 1-1. Sample Operations Security Estimate

1-14. *Visualize.* As commanders begin to understand an operational environment, they visualize a desired end state and potential solutions to solve the problem. Potential solutions will contain essential elements of friendly information that require protection.

1-15. *Describe.* OPSEC-related responsibilities that facilitate shared understanding and purpose include—

- Approving unit OPSEC documentation (threat assessment, essential elements of friendly information list, vulnerability assessment, risk assessment, and measures and countermeasures).
- Integrating measures and countermeasures into plans and SOPs.
- Approving intelligence and essential elements of friendly information support requirements within the unit or request assistance from higher headquarters. Designate an OPSEC planner.

1-16. *Direct.* OPSEC-related responsibilities that inform commander's intent, set achievable objectives, and issue clear tasks include—

- Directing implementation of measures and countermeasures to support ongoing and projected operations.
- Integrating measures and countermeasures into plans and SOPs and direct (via orders, directives, and policies) unit personnel to protect essential elements of friendly information.
- Directing subordinate units to establish an essential elements of friendly information list, develop measures and countermeasures, and provide feedback on the essential elements of friendly information.

- Ensuring a process is in place to dispose of essential elements of friendly information in a manner that prevents inadvertent disclosure or reconstruction of the material.

1-17. *Lead.* OPSEC-related responsibilities that help commanders provide purpose, direction, and motivation to subordinate commanders, their staffs, and Soldiers include—

- Designating an OPSEC planner.
- Ensuring that the unit OPSEC plan addresses personnel with access to sensitive essential elements of friendly information and that a process is in place to dispose of essential elements of friendly information in a manner that prevents inadvertent disclosure or reconstruction of the material.
- Instructing unit personnel not to publicly reference, disseminate, confirm, publish, or further propagate essential elements of friendly information previously compromised.
- Maintaining OPSEC in Family Readiness Support Assistant and Family Readiness Group activities and in unit contracting activities.
- Ensuring the unit public affairs review includes an OPSEC review and the official information intended for public release or made available through social media does not compromise unit essential elements of friendly information.

1-18. *Assess.* OPSEC-related responsibilities that help commanders anticipate, and adapt the force to, changing circumstances include—

- Establishing OPSEC as an evaluation objective for operations.
- Ensuring OPSEC documents are reviewed, OPSEC reviews are documented, and annual OPSEC reports are submitted to higher headquarters at least annually.

1-19. The unit OPSEC planner is responsible for a variety of activities requiring extensive collaboration with the staff to fully implement supportive measures and countermeasures. For example, the OPSEC planner consults with the assistant chief of staff, intelligence (G-2), on matters pertaining to the status of enemy or adversary intelligence collection capabilities and the ability of these forces to collect against unit essential elements of friendly information and indicators. The staff military deception officer works with the OPSEC planner to ensure measures and countermeasures are timed and implemented in a manner that assists the unit in presenting false indicators that confuse threat forces or make unit intentions harder to interpret. Various other staff officers collaborate with the OPSEC planner on placing and employing decoys, camouflage, and other concealment used to mask or hide unit indicators of activity, personnel, and equipment. Operations officers routinely consult with the OPSEC planner before the initiation of rehearsals to mitigate potential indicators of pending unit intentions or activities.

1-20. The most frequent staff coordination responsibilities for the OPSEC planner are shown in table 1-2 on page 1-6

Table 1-2. Examples of Operations Security Planner Staff Coordination Responsibilities

Type of Responsibility	*OPSEC Planner Staff Coordination Responsibilities*
Advise	• Commander and staff on current status and any changes to the unit's OPSEC posture. • Commander and staff on the means available to the unit to prevent the disclosure of EEFIs.
Recommend	• EEFIs for commander approval. • To commander and staff measures and countermeasures to eliminate or reduce known or perceived unit OPSEC vulnerabilities.
Perform	• Periodic unit OPSEC reviews. • Unit OPSEC training. • Unit OPSEC assessments of measures and countermeasures. • Unit OPSEC reviews of documents, information-systems logs, and news releases for compromises of commander-approved EEFIs. • Searches of open-source media, blogs, and other websites for unit EEFIs.
Prepare	• Unit OPSEC estimate. • Unit OPSEC SOP. • Appendix 3 (OPSEC) to Annex E (Protection) of the operation order.
Determine	• Length of time EEFIs need protection.
Publish	• Commander-approved unit EEFIs.
Synchronize	• Implementation of measures and countermeasures with OPSEC planners at higher, adjacent, and subordinate units.
Participate	• In the unit protection working group where OPSEC issues and concerns are raised.
EEFI essential element of friendly information OPSEC operations security SOP standard operating procedure	

Chapter 2

The Staff Operations Security Process

2-1. The unit OPSEC planner employs the staff OPSEC process, a framework designed to assist OPSEC planners. The OPSEC process can be conducted as follows:

- Identify essential elements of friendly information—identify essential elements of friendly information associated with unit operations, capabilities, activities, limitations, and intentions requiring protection.
- Analyze threats—analyze the vulnerability of essential elements of friendly information to exposure and exploitation by enemy and adversary information and intelligence gathering, production, and dissemination.
- Evaluate vulnerabilities—evaluate unit practices, tactics, routines, and information sources that are or may be susceptible to enemy, adversary, or threat exploitation through deliberate, unauthorized, or inadvertent exposure of essential elements of friendly information associated with unit operational capabilities, activities, limitations and intentions.
- Assess risk—assess the readiness and suitability of essential elements of friendly information protective measures available to the unit that must be implemented to prevent enemy, adversary, or threat intelligence collection activities directed against the unit and its personnel.
- Recommend measures and countermeasures—recommend protective measures that must be implemented as part of unit operations to protect essential elements of friendly information from enemy, adversary, or threat intelligence collection activities.

2-2. The staff OPSEC process is accomplished within the military decisionmaking process (MDMP). The OPSEC planner provides planning guidance and tasking recommendations for the unit staff elements and unit personnel overall. Each staff element identifies essential elements of friendly information, protection responsibilities, and vulnerabilities, and provides them to the OPSEC planner. OPSEC planning guidance is usually in the form of an OPSEC estimate and includes the following main items:

- An estimate of probable enemy knowledge of unit operations (see table 1-1, page 1-4).
- A preliminary list of essential elements of friendly information.
- A summary of enemy intelligence collection capabilities.
- A list of OPSEC indicators by staff function.
- A list of measures and countermeasures to implement immediately and additional measures requiring consideration.

2-3. By incorporating OPSEC into planning early on, unit operations become more effective during execution. It is important to note that frequently the enemy relies on visibly observable indicators that over time have been linked with unit activities known to be a prelude to or reaction to operations. Reducing, masking, or deflecting attention from potential indicators provides a first-level measure in protecting potential essential elements of friendly information.

IDENTIFY ESSENTIAL ELEMENTS OF FRIENDLY INFORMATION

2-4. Units can produce a great deal of information during the course of an operation that can reveal a unit's capabilities, activities, limitations and intentions. Protecting all information from compromise or exploitation by a dedicated enemy, adversary, or threat is unrealistic, even under the most ideal circumstances. Properly implemented measures and countermeasures strive to protect essential elements of friendly information that must be protected to ensure operational success. The unit OPSEC planner, with assistance provided by the unit staff, recommends potential essential elements of friendly information for the commander's approval.

2-5. In OPSEC, essential elements of friendly information are unclassified and therefore not subject to the stringent protections provided to classified information. However, essential elements of friendly information can, based on source, compilation, or collation, compromise and even expose classified information to exploitation by a determined enemy.

2-6. The OPSEC planner can use several sources to determine essential elements of friendly information. The unit commander issues operational guidance, direction, and intent to the staff. In addition to security classification guidance, the intelligence staff officer provides information on the enemy, adversary, or threat force status, intent, and capability including information and intelligence collection activities directed against the unit. The operations staff officer provides an overview of current and future operations. Other primary staff officers provide information detailing status, capabilities, activities, limitations, and intentions associated with unit systems, platforms, and processes under their direct control. Higher headquarters issues OPSEC guidance. Subordinate units develop and forward recommendations for essential elements of friendly information to higher echelons. Higher echelons consolidate and incorporate the recommendations with their own essential elements of friendly information, as appropriate, and subsequently issue consolidated list of essential elements of friendly information. Subordinate units strive to act upon and support the higher echelon consolidated essential elements of friendly information in addition to their unit-specific essential elements of friendly information.

Note. Many potential items associated with operations at the unit level can be considered essential elements of friendly information. Examples include, but are not limited to, the items shown in table 2-1 on page 2-3.

Table 2-1. Sample Essential Elements of Friendly Information

Information Type	*Sample Essential Elements of Friendly Information*
Communications	• Mission Command systems. • Communications site locations. • Communications limitations (such as weather, terrain, and equipment shortages).
Counterintelligence	• Number and disposition of counterintelligence assets available to the unit. • Identification and location of counterintelligence elements and activities supporting the unit. • Identification of local personnel that may be assisting unit-assigned counterintelligence forces.
Courses of action	• Unit COAs being planned or under consideration. • Unit COAs that cannot be undertaken or executed.
Deception	• Unit support to planned military deceptions. • Ongoing deception operations. • Unit support to interagency involvement in deception operations. • Identity of unit elements performing or participating in military deception activities. • Unit leadership or personnel vulnerable to enemy deception activities.
Forces	• Unit forces earmarked for possible COAs. • Readiness levels of the unit. • Current and projected unit locations.
Host nation or multinational force partners	• Host nation support to the unit. • Information exchange agreements and protocols between the unit and host nation or multinational force partners. • Vulnerabilities that could be exploited to reduce or eliminate host nation or multinational force support.
Intelligence	• Intelligence collection, analysis, and dissemination capabilities available to the unit. • Unit surveillance and reconnaissance capabilities available to or embedded in the unit. • Locations of unit intelligence, surveillance, and reconnaissance capabilities supporting the unit. • Intelligence, surveillance, and reconnaissance operations supporting the unit. • Vulnerabilities to exploitation or destruction of unit intelligence, surveillance, and reconnaissance capabilities.
Locations	• Specific locations of unit exercises and operations. • Specific locations of participating forces. • Specific projected unit locations. • Alternate unit locations.

Table 2-1. Sample Essential Elements of Friendly Information (continued)

Information Type	*Sample Essential Elements of Friendly Information*
Logistics	• Logistic posture of unit forces. • Speed of deployment or redeployment of unit forces. • Unit lines of communications. • Unit-associated locations of storage depots, ports, and airfields. • Vulnerabilities to interdiction of the lines of communication. • Contents of unit pre-positioned stocks and significant restructuring of unit pre-positioned stocks.
Maintenance	• Maintenance and salvage capabilities of the unit. • Support and sustainment expectations for the unit. • Vulnerabilities to attack associated with maintenance support and sustainment capabilities.
Medical	• Unit casualty figures, both actual and projected. • Very important persons being treated by unit medical treatment elements. • Unit medical supplies required (such as vaccines and blood products). • Shortages in unit medical military occupational specialties and personnel. • Identification of projected unit medical personnel and team deployments. • Identified medical vulnerabilities of unit personnel and capabilities.
Military information support operations	• Intended psychological warfare and subversion operations. • Plans to exploit enemy vulnerabilities. • Ongoing and planned operations. • Interagency support provided to the unit or to supporting military information support operations elements. • Military information support operations themes and objectives. • Vulnerabilities of the unit to psychological warfare and subversion.
Mission command	• Unit command arrangements for executing COA. • Current or future locations of unit commanders. • Current or future command post locations. • Command post vulnerabilities.
Mission command information systems	• Information protection measures and procedures implemented at the unit level. • Electromagnetic spectrum protections implemented to protect unit wireless mission command communications systems. • Defensive cyberspace operations implemented to protect unit networked information systems. • Unit-specific identified vulnerabilities associated with mission command systems at operational locations.
Policies or rules of engagement	• Those governing the use of weapons and electronic or acoustic warfare systems.

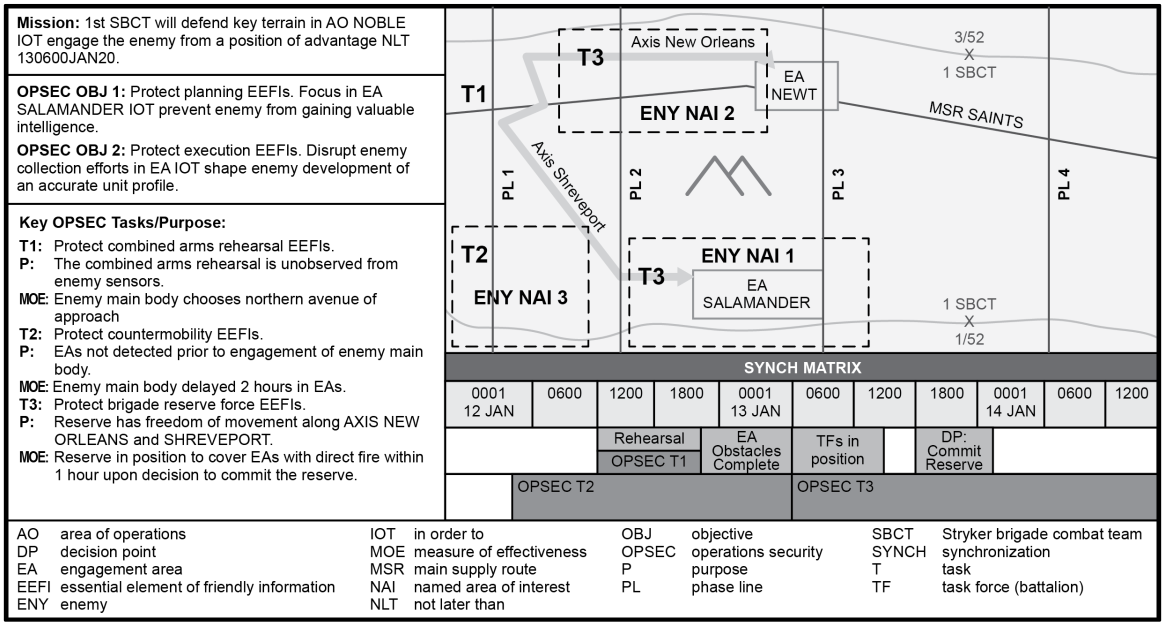
Table 2-1. Sample Essential Elements of Friendly Information (continued)

Information Type	*Sample Essential Elements of Friendly Information*
Special operations forces and unconventional warfare	• Intended sabotage and direct action mission targets. • Enemy vulnerabilities planned for exploitation. • Unit capabilities supporting unconventional warfare operations. • SOF team deployment dates, deployment sites, and support timelines. • Number of SOF teams and personnel in the area of operations. • Unit support to SOF teams and unit elements associated with SOF teams and personnel.
Supplies	• Supply levels available for immediate support and period of combat sustainment with those supplies. • Pre-positioned supply sites. • Critical item shortages (in all classes). • Limitations to resupply capacity. • Demand level for Class IX items.
Vulnerabilities	• Defensive dispositions. • Sensors and other capabilities to detect attack. • Vulnerabilities to attack. • Units, weapons, and weapons systems. • Protection, security forces, or security plans.
Weapons	• Specific characteristics and capabilities of unit weapons and electronic systems. • Unit tactics, techniques, and procedures for using various weapons. • Indicators of unconventional weapons employment. • Indicators of new weapons employment. • Vulnerabilities and limitations in unit weapons and weapons systems.
COA course of action SOF special operations forces	

ANALYZE THREATS

2-7. The OPSEC planner compares essential elements of friendly information to known or perceived enemy information and intelligence collection capabilities. When deployed, units should consider that enemy forces conduct active and deliberate collection efforts against the unit where the intent is to observe, acquire, and exploit indicators and information sources that expose unit capabilities, activities, limitations and intentions. OPSEC indicators, actions and open-source information related to the unit and unit operations can be detected, analyzed, and interpreted by enemy forces and ultimately lead to unauthorized disclosure of unit-specific essential elements of friendly information.

2-8. With assistance provided by the unit's intelligence staff and other staff elements, the OPSEC planner examines each part of the operation to find actions or information that provide indicators in areas such as personnel, logistics, communications, movement activities, and aviation. Subsequent comparisons are performed to determine whether the indicator can be exploited by enemy intelligence collection capabilities. A vulnerability exists when enemy forces can collect an indicator of essential elements of friendly information, correctly analyze the information, make a decision, and take timely action to adversely influence, degrade, or prevent unit operations. One method successfully used by units to mitigate known or perceived information vulnerabilities is to develop a scheme of OPSEC. The scheme of OPSEC synchronizes OPSEC tasks with the mission timeline and provides a tool for the commander to identify information and indicator concerns that must be protected at each interval. Although no set format exists for a scheme of OPSEC, figure 2-1 is one example.



Mission: 1st SBCT will defend key terrain in AO NOBLE IOT engage the enemy from a position of advantage NLT 130600JAN20.

OPSEC OBJ 1: Protect planning EEFIs. Focus in EA SALAMANDER IOT prevent enemy from gaining valuable intelligence.

OPSEC OBJ 2: Protect execution EEFIs. Disrupt enemy collection efforts in EA IOT shape enemy development of an accurate unit profile.

Key OPSEC Tasks/Purpose:

T1: Protect combined arms rehearsal EEFIs.
P: The combined arms rehearsal is unobserved from enemy sensors.
MOE: Enemy main body chooses northern avenue of approach
T2: Protect countermobility EEFIs.
P: EAs not detected prior to engagement of enemy main body.
MOE: Enemy main body delayed 2 hours in EAs.
T3: Protect brigade reserve force EEFIs.
P: Reserve has freedom of movement along AXIS NEW ORLEANS and SHREVEPORT.
MOE: Reserve in position to cover EAs with direct fire within 1 hour upon decision to commit the reserve.

SYNCH MATRIX

0001 12 JAN	0600	1200	1800	0001 13 JAN	0600	1200	1800	0001 14 JAN	0600	1200
		Rehearsal OPSEC T1		EA Obstacles Complete	TFs in position		DP: Commit Reserve			
	OPSEC T2				OPSEC T3					

AO	area of operations	IOT	in order to	OBJ	objective	SBCT	Stryker brigade combat team
DP	decision point	MOE	measure of effectiveness	OPSEC	operations security	SYNCH	synchronization
EA	engagement area	MSR	main supply route	P	purpose	T	task
EEFI	essential element of friendly information	NAI	named area of interest	PL	phase line	TF	task force (battalion)
ENY	enemy	NLT	not later than				

Figure 2-1. Sample Scheme of Operations Security

2-9. The scheme of OPSEC can reveal indicators available for threat forces to exploit. A comparison of the enemy's ability to collect against the unit and the indicators associated with the mission timeline determined by the staff reveals actual and potential unit vulnerabilities. The combination of indicators that the enemy is expected to look for along with potential courses of action can reveal one or more named areas of interest. The enemy may choose to observe these named areas of interest with reconnaissance assets. This information is valuable in developing OPSEC measures and countermeasures.

2-10. Unit OPSEC planners can use the following series of questions to help them as they work to refine a consolidated unit essential elements of friendly information list:

- What essential elements of friendly information are likely known by enemy forces?
- Can those essential elements of friendly information be provided a measure of protection?
- What unit activities may create indicators to essential elements of friendly information currently unknown by enemy forces?
- What indicators can enemy forces actually collect (this depends on the capabilities of the enemy's intelligence system)?
- What indicators are the enemy likely to use to the disadvantage of the unit?
- Which indicators can influence enemy decision makers to the benefit of unit operations?

ANALYZE VULNERABILITIES

2-11. Unit OPSEC planners strive to mitigate unit vulnerabilities by applying available measures and countermeasures. The most desirable measures and countermeasures provide maximal protection at minimal cost to operational effectiveness and efficiency. Recommended measures and countermeasures fall into three categories: unit-level action control, disruption of enemy collection, and counteranalysis.

ACTION CONTROL

2-12. Measures to control unit activities can eliminate or reduce to an acceptable level operational indicators or the vulnerability of actions to exploitation by enemy intelligence systems. Unit OPSEC planners select the actions required (for example, OPSEC reviews), decide whether or not to execute the actions, and impose restraints on actions (for example, paper shredding and trash control and mandatory use of secure communications or communications blackouts).

Disruption of Enemy Collection

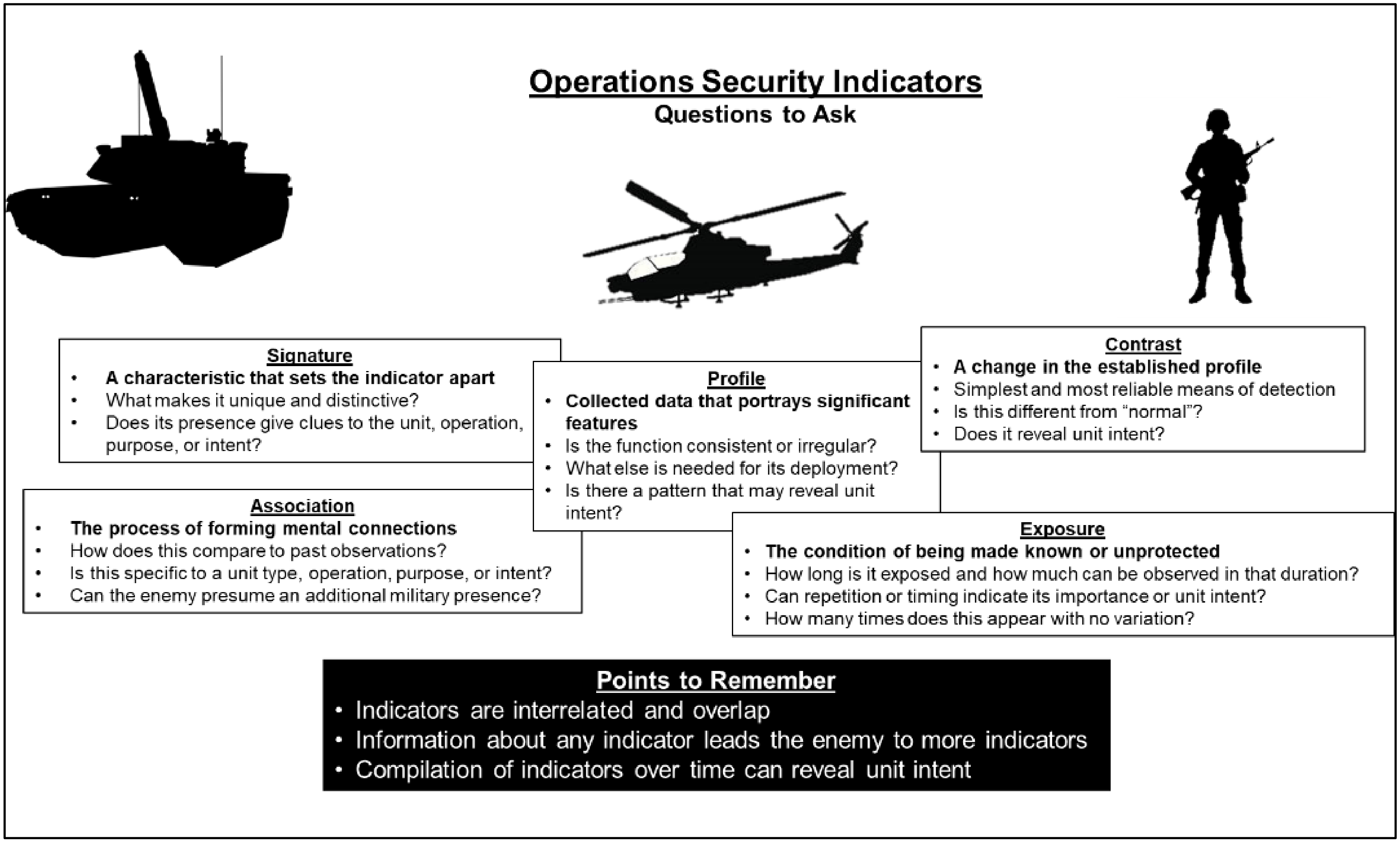
2-13. Unit OPSEC planners propose countermeasures to disrupt enemy collection against the unit or prevent the threat's ability to recognize indicators when collected materials are processed. Examples of countermeasures include diversions, camouflage, concealment, jamming, deterrence, police powers, and force against enemy information gathering and processing capabilities.

Counteranalysis

2-14. Unit OPSEC planners employ counteranalysis directed at enemy analysts to prevent the enemy from accurately interpreting indicators during its analysis of collected material. Often, the OPSEC planner relies on the use of deception countermeasures to confuse and distract the enemy analysts.

2-15. Unit observable indicators are an important facet of an OPSEC-focused vulnerability analysis. Indicators reveal information and data that the enemy analyst can piece together to develop an intelligence estimate of the unit. Indicators are data derived from open sources; from detectable unit actions that the enemy pieces together or interprets to reach conclusions; or from official estimates concerning unit capabilities, activities, limitations, and intentions. Based on the intelligence estimate that the enemy develops, which is further reinforced by detectable unit indicators, the enemy formulates and develops a perception of the unit and its ability to conduct operations in a given area of operations.

2-16. The OPSEC planner seeks to influence and manipulate enemy perceptions by modifying and adjusting detectable unit indicators. These efforts delay or diminish enemy attempts to develop an accurate intelligence estimate or profile of the unit. Indicators are grouped into one of five possible categories: signature, association, profile, contrast, or exposure (see figure 2-2 on page 2-8).



Operations Security Indicators

Questions to Ask

Signature

- **A characteristic that sets the indicator apart**
- What makes it unique and distinctive?
- Does its presence give clues to the unit, operation, purpose, or intent?

Profile

- **Collected data that portrays significant features**
- Is the function consistent or irregular?
- What else is needed for its deployment?
- Is there a pattern that may reveal unit intent?

Contrast

- **A change in the established profile**
- Simplest and most reliable means of detection
- Is this different from "normal"?
- Does it reveal unit intent?

Association

- **The process of forming mental connections**
- How does this compare to past observations?
- Is this specific to a unit type, operation, purpose, or intent?
- Can the enemy presume an additional military presence?

Exposure

- **The condition of being made known or unprotected**
- How long is it exposed and how much can be observed in that duration?
- Can repetition or timing indicate its importance or unit intent?
- How many times does this appear with no variation?

Points to Remember

- Indicators are interrelated and overlap
- Information about any indicator leads the enemy to more indicators
- Compilation of indicators over time can reveal unit intent

Figure 2-2. Categories of Operations Security Indicators

Signature

2-17. The indicator's signature is a characteristic that serves to set the indicator apart. A signature makes the indicator identifiable or causes it to stand out. Uniqueness and stability are properties of a signature. Uncommon or unique features reduce the ambiguity of an indicator. An example is the unique design of the M-1-series main battle tank. Its visual signature cannot be mistaken from most tanks. A unique visual signature minimizes the number of other indicators that the enemy must observe to confirm its significance. An indicator's signature stability, which implies constant or stereotyped behavior, allows the enemy to predict intentions. Varying behavior decreases the signature's stability and thus increases the ambiguity of the enemy's observations. Procedural features are an important part of any indicator's signature and may provide the greatest value to an enemy. These features identify how, when, and where the indicator occurs and what part it plays in the overall scheme of operations and activities.

Association

2-18. Association is the process of forming mental connections to an indicator. It is the key to interpretation. An enemy compares current data with previously gathered information to identify possible relationships. Continuity of actions, objects, or other indicators, which register as patterns, provides another association. For example, the presence of special operations aviation aircraft, such as the MH-6, MH-60, and MH-47, may be indicators of other special operations forces operating in the area. Certain items of equipment particular to specific units are indicators of the potential presence of related equipment. For instance, the sighting of an M-88A2 Hercules Recovery Vehicle likely indicates the presence of an armored unit equipped with M1A2-series tanks, as the M-88A2 is rated to recover and tow the M1A2-series tanks. Such continuity can result from repetitive practices or sequencing instead of from planned procedures. When detecting some components of symmetrically-arrayed organizations, the enemy can assume the existence of the rest. As another example, the adversary would suspect the presence of an entire infantry battalion when intelligence detects the headquarters company and one line company. When evaluated as a whole, the pattern can be a single indicator, which simplifies the enemy's analysis.

Profile

2-19. A profile is accumulated data that portray the significant features of an indicator. Profiles are linked to functional activity, which has a profile comprising unique indicators, patterns, and associations. The profile of an aircraft deployment, for example, may be specific to the aircraft type or mission, as in the special operations aviation example in paragraph 2-18. This profile, in turn, has several sub-profiles for the functional activities needed to deploy the particular mission aircraft (for example, fuels, avionics, munitions, communications, air traffic control, supply, personnel, and transportation). If a functional profile does not appear to change from one operation to the next, it is difficult for an enemy to interpret. However, if it is distinct, the profile may be the key or only indicator needed to understand the operation. Unique profiles reduce the time needed to make accurate situational assessments. They are primary warning tools because they provide a background for contrasts, as described in paragraph 2-20.

Contrast

2-20. Contrast is the change in an indicator's established profile. The key to obtaining the contrast of an indicator lies in how it differs from what has been shown previously. Contrasts are the simplest and most reliable means of detection because they only need to be recognized, not understood. One question prompts several additional ones concerning contrasts in profile. The nature of the indicator's exposure is an important aspect when seeking profile contrasts. For example, if the adversary identifies items specific to special operations aviation at an airfield, this will contrast with what is "normal" at the airfield and will indicate the deployment of special operations aircraft to the airfield without having actually observed them.

Exposure

2-21. Exposure is the condition of being presented to view or made known—the condition of being unprotected. For an OPSEC indicator, exposure increases according to the duration, repetition, and timing of its appearance. The exposure of an indicator often reveals its relative importance and meaning. Limited duration and repetition reduces detailed observation and associations. An indicator that appears for a short time will likely fade into the background of insignificant anomalies. An indicator that appears over a long period of time, however, becomes part of a profile. Indicators exposed repeatedly present the biggest danger. Operations conducted the same way several times with little or no variation provide an adversary the information needed to determine where, when, how, and with what to attack. Repetitive operations cost many lives in wartime.

SAMPLE INDICATORS

2-22. Indicators that unit OPSEC planners may consider as they review their individual unit OPSEC requirements are shown in table 2-2.

Table 2-2. Sample Indicators

Type of Indicator	*Sample Indicator*
Administrative	• Temporary duty orders. • Conferences. • Transportation arrangements. • Billeting arrangements. • Medical care. • Schedules. • Plans of the day. • Block leave for large groups or entire units. • Reserve mobilization. • Changes to daily schedules. • Change of mail addresses or arrangements to forward mail on a large scale. • Runs on the Post Exchange for personal articles, such as personal radios. • Emergency personnel requisitions and requests for critical skills. • Emergency recall of personnel on leave and pass.
Communications	• Voice and data (telephone, cell phone, wireless) transmissions between unit personnel in an operation. • Establishment of unit command nets. • Changes in message quantity to secure systems, such as increased radio, email, and telephone traffic from headquarters. • Units reporting to new commanders. • Identification of units, tasks, or locations in unsecure transmissions. • Increased communications checks between units or organizations. • Press conferences or an increase in press releases from the public affairs office. • Unnecessary or unusual increases in reporting requirements. • Sudden imposition of communications security measures, such as radio silence. • Appearance of new radio stations in a net. • Communications exercises. • Appearance of different cryptographic equipment or materials. • Increase in unofficial use of commercial email services. • Unofficial use of instant messenger and chat forums. • Increased family readiness group and family readiness support assistant posture.

Table 2-2. Sample Indicators (continued)

Type of Indicator	*Sample Indicator*
Emissions other than communications	• Radar and navigational aids that reveal unit location or identity. • Normal lighting in a blackout area. • Loud unit vehicle or personnel movements. • Smoke and other odors.
Engineering	• Radar and navigational aids that reveal unit location or identity. • Normal lighting in a blackout area. • Loud unit vehicle or personnel movements. • Smoke and other odors.
Intelligence, counterintelligence, and security	• Concentrated unit reconnaissance in a particular area. • Embarking or moving special equipment. • Recruitment of personnel with particular language skills. • Routes of reconnaissance vehicles. • Sensor drops in target area. • Increased activity of friendly agent nets. • Increased ground patrols. • Unusual or increased requests for meteorological or oceanographic information. • Unique or highly visible security to load or guard special munitions or equipment. • Enemy radar, sonar, or visual detection of friendly units. • Unit identification through, for example, communications security violations or physical observation of unit symbols. • Trash and recycle bins that contain essential elements of friendly information.
Logistics	• Volume and priority of requisitions. • Package or container labels that show the name of an operation, program, or unit designation. • Pre-positioning equipment or supplies. • Procedural disparities in requisitioning and handling. • Accelerated maintenance of weapons and vehicles. • Presence of technical representatives. • Unusual equipment modification. • Increased motor pool activities. • Test equipment turnover. • Special equipment issue. • Stockpiling petroleum, oil, lubricants, and ammunition. • Upgraded lines of communication. • Delivery of special or uncommon munitions. • New support contracts or host nation agreements. • Arranging for transportation and delivery support. • Requisitions in unusual quantities to be filled by a particular date.

Table 2-2. Sample Indicators (continued)

Type of Indicator	*Sample Indicator*
Medical	• Stockpiling plasma and medical supplies. • Movement of deployable medical sets. • Immunization of units with area-specific and time-dependent vaccines. • Identifying special medical personnel and teams deploying to specific areas.
Operations, plans, and training	• Changes in post defense readiness condition, force protection condition, or information condition. • Movement of unit personnel into position for operations. • Abnormal dispersions or concentrations of unit personnel. • Deviations from routine training. • Rehearsals and drills for a particular mission. • Exercises and training of unit personnel in pre-designated areas. • Repeating operations the same way, same time, same route, or in same area. • Fixed schedules and routes. • Standard reactions to hostile acts. • Standardizing maneuvers or procedures. • Standardizing unit personnel mixes and numbers to execute particular missions down to squad-level operations. • Changing guards at fixed times. • Appearance of special purpose units (such as bridge companies, pathfinders, explosive ordnance detachments, SOF, and liaison teams). • Change in task organization or arrival of new attachments. • Artillery registration in new objective area. • Surge in food deliveries to planning staffs at major headquarters. • Unit and equipment deployments from normal bases.
SOF special operations forces	

ASSESS RISK

2-23. Assessing risk involves selecting optimal measures and countermeasures to implement. The unit OPSEC planner decides which, if any, measures and countermeasures to recommend for implementation and when to do so. The planner checks the interaction of measures and countermeasures to ensure they protect essential elements of friendly information while not inadvertently revealing other indicators. Staff coordination is essential.

2-24. The unit OPSEC planner then recommends to the commander the measures and countermeasures required to protect unit essential elements of friendly information. The OPSEC planner also prepares responses to questions likely to be asked, such as—

- If the measure or countermeasure is implemented, what is the likely impact on operational effectiveness?
- If the measure or countermeasure is implemented, what is the potential impact to other units?
- If the measure or countermeasure is successful, what is the potential impact on future missions?
- If the measure or countermeasure is not implemented, what is the risk to mission success or effectiveness?
- If the measure or countermeasure does not work, what is the probable risk to mission success?

2-25. Commanders decide and approve measures and countermeasures. Occasionally, commanders decide on a no-measures alternative. This might occur when the OPSEC process determines that specific essential elements of friendly information require no protection or that the costs of protection significantly outweigh risks. Ultimately, those decisions rest with commanders. Commanders balance the risk of operational failure against the cost of implementing the measures and countermeasures. The OPSEC planner must document all recommendations, whether they are approved or disapproved, for future reference.

RECOMMEND MEASURES AND COUNTERMEASURES

2-26. Under routine circumstances, the unit OPSEC planner implements the commander's approved measures and countermeasures, which unit personnel incorporate as part of operations. The OPSEC planner selects at least one tentative measure or countermeasure for each identified unit vulnerability. In some cases, a planner considers deception and cover as viable measures at the unit tactical level. Some measures and countermeasures may apply to more than one vulnerability. A planner specifies who, when, where, how, and for how long the measure or countermeasure is in effect.

2-27. The unit OPSEC planner documents measures and countermeasures in Appendix 3 (Operations Security) to Annex E (Protection) of an operation order (OPORD). For more information on OPORD annexes and appendixes, see FM 6-0. Additional information on measures and countermeasures is available through input provided to unit OPSEC plans, SOPs, and other memoranda issued in either hard copy or by electronically-transmitted messages. Documentation of measures and countermeasures incorporated into operations is especially important when emphasizing which measures and countermeasures require immediate action. Documentation also ensures unit personnel fully understand their roles and responsibilities in current and future operations.

2-28. The OPSEC planner prepares and delivers staff briefings to unit planners, operators, and support personnel. Planners stress that measures and countermeasures are command-directed actions executed by individuals who must understand their responsibilities and the adverse results of a failure to maintain effective OPSEC throughout the operation. Upon receipt of the OPSEC planner's guidance and tasking instructions, unit personnel implement the command-directed measures and countermeasures. The OPSEC planner evaluates the effectiveness of the directed measures and countermeasures during execution.

2-29. Application of measures and countermeasures is a continuous process that includes evaluating intelligence and counterintelligence reports, public media disclosures, website reviews, integrated systems security monitoring, and feedback reports (such as OPSEC assessments and surveys) on measures and countermeasures. In addition to evaluating the effectiveness of measures and countermeasures, the OPSEC planner recommends adjustments to improve the effectiveness of existing measures and countermeasures, and recommends new measures and countermeasures where new vulnerabilities develop. Table 2-3 on page 2-14 lists examples of measures and countermeasures.

Table 2-3. Sample Measure and Countermeasures

Type of Measure	*Sample Countermeasures*
Administrative	• Limit or avoid bulletin board plan of the day or planning schedule notices that reveal when events will occur. • Conceal supply requests and actions and arrangements for services that reveal preparations for activity. • Conceal the issuance of orders, movement of specially-qualified unit personnel, and the installation of special capabilities. • Control trash dumping or other housekeeping functions to conceal the locations and identities of unit elements and personnel. • Destroy (for example, burn or shred) paper, including unclassified information, to prevent the inadvertent disposal of classified and sensitive information. • Follow normal leave and pass policies to the maximum extent possible before an operation starts to preserve an illusion of normalcy. • Ensure personnel discreetly prepare for their family's welfare in their absence and their families are sensitized to their potential abrupt departure. • Maximize use of security screening of local national hires and minimize their access and observation opportunities in the unit. • Randomize security in and around the installation or camp to prevent setting a pattern or an observable routine. • Perform random, unannounced, internal identity and security inspections.
Combat action	• Use force against enemy intelligence and information collection and processing capabilities. • Prevent enemy efforts to collect against unit personnel and operations.
Deception	• Employ deception in support of OPSEC to distract enemy or foreign intelligence entities away from, or provide cover for, unit operations and supporting activities. • Employ deception to prevent inadvertent or unauthorized disclosure of classified information, EEFIs, and sensitive unclassified information. • Employ OPSEC in support of deception to identify possible conduits for passing deceptive information to the enemy. • Employ OPSEC in support of deception to protect against inadvertent or unintentional outcomes.

Table 2-3. Sample Measures and Countermeasures (continued)

Type of Measure or Countermeasure	*Sample Measure and Countermeasures*
Operations and logistics	• Randomize the performance of functions and operational missions. Avoid repetitive or stereotyped tactics and procedures for conducting operations or activities in terms of time, place, event sequencing, formations, and mission command arrangements. • Employ force dispositions and mission command arrangements that conceal the location, identity, and command relationships of unit elements. • Conduct support activities in a way that will not reveal intensifying preparations before initiating operations. • Ensure the transportation of supplies and personnel to the unit is accomplished in a way that conceals the location and identity of the unit. • Operate unit aircraft at varying altitudes and use random flight routes. • Operate to minimize the reflective surfaces that unit weapons systems present to radar and sonar. • Use darkness to mask unit deployments. • Approach an objective "out of the sun" to prevent detection. • Randomize unit convoy routes, departure times, speeds, and so forth. • Randomize unit patrolling patterns (such as start times, locations, and number of personnel in a patrol). • Randomize use of unit-designated landing zones or pick-up points. • Randomize use of unit approach (aircraft) or route (vehicle) into and out of an area. • Randomize the locations of unit overwatch, sniper, communications, medical evacuation, and support positions. • Vary small-unit patrol formations. Do not set patterns.
Technical	• Use radio communications emission controls, low probability of intercept techniques, traffic flow security, ultrahigh frequency relay via aircraft, burst transmission technologies, and secure phones, landlines, and couriers. • Limit use of high-frequency radios and directional super-high-frequency transponders. • Control radar emissions and operate at reduced power. • Mask unit emissions from radar or visual detection by use of terrain (such as hills and mountains). • Maintain noise discipline, operate at reduced power, proceed at slow speeds, and turn off selected equipment. • Use camouflage, smoke, background noise, added sources of heat or light, paint, or weather. • Use deceptive radio transmissions. • Use decoy radio or emission sites.
EEFI essential element of friendly information OPSEC operations security	

This page intentionally left blank.

Chapter 3

Operations Security and the Military Decisionmaking Process

3-1. The *military decisionmaking process* is an iterative planning methodology to understand the situation and mission, develop a course of action, and produce an operation plan or order (ADP 5-0). Also called MDMP. The unit OPSEC planner participates as part of staff during the MDMP, which ensures OPSEC is fully integrated into all plans and orders (see table 3-1 on page 3-2).

3-2. The initial step of the MDMP is receipt of mission. During this step, the OPSEC planner begins identifying essential elements of friendly information and analyzing the enemy's capabilities, with special emphasis on the enemy's ability to conduct reconnaissance, surveillance, intelligence gathering, and information collection directed at the unit. The unit commander's initial assessment and guidance may result in preliminary essential elements of friendly information or guidance to assist the OPSEC planner. If not already established by the commander, the OPSEC planner identifies initial essential elements of friendly information based on the unit OPSEC estimate and assessment. The unit assistant chief of staff, operations, or the battalion or brigade operations staff officer disseminates initial essential elements of friendly information in the initial warning order. The OPSEC planner provides initial essential elements of friendly information to the assistant chief of staff, intelligence, or the battalion or brigade intelligence staff officer for consideration in initial intelligence preparation of the battlefield. OPSEC information requirements concerning the enemy's capability to collect essential elements of friendly information are submitted to the unit assistant chief of staff, operations, or the battalion or brigade operations staff officer for inclusion in the initial reconnaissance and surveillance tasking. Once the essential elements of friendly information are identified, and during the remaining steps of the MDMP, the OPSEC planner focuses on protecting this information.

3-3. As the MDMP continues to the next step of mission analysis, the OPSEC planner conducts an analysis of the threat. The primary product of mission analysis for the OPSEC planner is OPSEC planning guidance, which outlines the essential elements of friendly information resulting from the threat analysis. Once developed, OPSEC planning guidance is applied throughout the MDMP and serves as the blueprint for subsequent OPSEC planning. The OPSEC planning guidance defines the essential elements of friendly information, taking into account unit and enemy goals, probable enemy knowledge, unit deception objectives, and enemy collection capabilities. The guidance also outlines provisional measures and countermeasures. As mission analysis proceeds, the OPSEC planner refines the initial essential elements of friendly information, continues to analyze the enemy, initiates a preliminary analysis of unit vulnerabilities, and conducts a risk assessment. OPSEC planning guidance is included in successive MDMP products, to include the commander's guidance and the warning order. OPSEC planner actions to analyze enemy and unit vulnerabilities correspond to risk management steps to identify and assess hazards.

3-4. Upon receipt of input from unit staff, and in particular the information operations element, the OPSEC planner reviews and refines essential elements of friendly information. Refinement continues following intelligence preparation of the battlefield and the determination of specified, implied, and essential tasks. The OPSEC planner participates in intelligence preparation of the battlefield throughout the operation, providing input useful to determining the enemy's most dangerous and most likely use of collection assets directed against the unit.

3-5. During course of action (COA) development, the OPSEC planner analyzes vulnerabilities, which involves identifying essential elements of friendly information associated with each COA and with the assets critical to the operation. Products produced by the OPSEC planner during COA development include refined essential elements of friendly information; OPSEC vulnerabilities with associated risks; and measures and countermeasures. The OPSEC planner action to develop measures corresponds to the risk management action to develop controls. As each COA is developed, the OPSEC planner identifies and assesses indicators to determine whether any constitute likely OPSEC vulnerabilities. Using the risk assessment matrix found in ATP 5-19, table 1-1, the OPSEC planner determines the level of risk and probability for each vulnerability and vulnerability-related occurrence. The OPSEC planner develops measures and countermeasures for all OPSEC vulnerabilities and determines the residual risk associated with each. This information is recorded on DD Form 2977, *Deliberate Risk Assessment Worksheet.* See ATP 5-19 for a sample of the worksheet and guidance on managing risk within the conduct of operations. The OPSEC planner considers measures and countermeasures to protect OPSEC vulnerabilities in the following areas on table 3-1 on page 3-3:

- Administration.
- Civil-military operations.
- Electronic warfare.
- Logistics.
- Deception.
- Operations.
- Physical destruction.
- Public affairs.
- Technical.

Table 3-1. The Military Decisionmaking Process and the Operations Security Planner

	OPSEC Planner Key Points	*Input*	*Actions*	*Outputs*
Military Decisionmaking Process	**Receipt of Mission**	• Commander's initial guidance.	• Identify EEFIs. • Develop enemy assumptions.	• Initial EEFIs and enemy assumption analysis.
	Mission Analysis	• S-2/G-2 and S-3/G-3 analysis and products.	• Analyze threat. • Refine EEFIs per input from unit staff, chiefly IO element.	• Initial OPSEC planning guidance. • Refined enemy analysis.
	COA Development	• Commander's intent. • Approved EEFIs.	• Analyze vulnerabilities. • Identify indicators and vulnerabilities.	• Determine residual risk. • Establish provisional OPSEC measures and countermeasures.
	COA Analysis	• OPSEC measures and countermeasures test and evaluation criteria. • Updated assumptions and running estimates.	• Evaluate COAs and OPSEC measures and countermeasures. • Assess risk. • Apply OPSEC measures and countermeasures.	• Coordinate OPSEC measures and countermeasures. • Identify operational support needed. • Resulting EEFIs and indicators.
	COA Comparison	• COA analysis results. • Refine vulnerability analysis and risk assessment. • Decision points.	• Identify and analyze resulting indicators. • Determine residual risk for supportable COAs.	• Identify and test OPSEC measures and countermeasures. • COA recommendation.
	COA Approval	• Approved COA. • Updated assumptions. • Risk assessment results.	• Determine resources needed for approved COA. • Determine measures of effectiveness.	• Ensure orders and plans contain instructions to prepare, execute, and assess measures. • Prepare Appendix 3 (OPSEC) to Annex E (Protection) of the OPORD.
	Orders Production, Dissemination, and Transition	• Approved orders, plans.	• Monitor OPSEC effectiveness.	• Update EEFIs as needed.

COA	course of action	MDMP	military decisionmaking process
EEFI	essential element of friendly information	OPORD	operation order
G-2	assistant chief of staff, intelligence	OPSEC	operations security
G-3	assistant chief of staff, operations	S-2	battalion or brigade intelligence staff officer
IO	information operations	S-3	battalion or brigade operations staff officer

3-6. Additional coordination may be required based on the rules of engagement established for some measures and countermeasures. Coordination may include the following:

- Determining the effects some measures and countermeasures have on public affairs operations.
- Obtaining guidance on terminating measures and countermeasures.
- Obtaining guidance on declassification and public release of OPSEC-related activities.
- Obtaining administrative and logistical support for OPSEC tasks.

- Establishing OPSEC coordination measures and mission command measures.
- Establishing assessment (monitoring and evaluation) mechanisms.
- Submitting information operation information requirements and requests for information to support assessment of information operation tasks.
- Conducting OPSEC checks.
- Arranging input for after-action reports.
- Arranging support of OPSEC-related communications requirements.

3-7. COA analysis allows the OPSEC planner to test measures and countermeasures associated with each COA. During war games, commanders may modify COAs based on how events develop. The OPSEC planner determines whether modifications result in additional recommendations for essential elements of friendly information or OPSEC vulnerabilities, and, if so, recommends and documents further measures and countermeasures. OPSEC products for COA analysis for each COA include refined essential elements of friendly information; evaluation and test criteria for measures and countermeasures; OPSEC vulnerabilities; decision points for executing measures and countermeasures; operational support needed for measures and countermeasures; measures and countermeasures needed to support possible operations plans; and whether any measures and countermeasures require additional coordination.

3-8. War gaming each COA requires the OPSEC planner to evaluate each COA on its strengths, weaknesses, advantages, and disadvantages. The OPSEC planner considers costs associated with planned measures and countermeasures and the risk involved with implementing or not implementing them. The OPSEC planner also determines whether enemy capabilities and indicators revealed during the war game result in previously unidentified OPSEC vulnerabilities. If so, the OPSEC planner develops recommended measures and countermeasures to shield the newly identified vulnerabilities as well. The OPSEC planner works with the intelligence officer to obtain information that fills gaps in intelligence preparation of the battlefield.

3-9. COA comparison identifies additional opportunities to implement measures and countermeasures and reveals which COAs may be more supportable based upon available resources. Those determinations are included in the OPSEC planner's recommendations to the commander during COA approval. In COA comparison, structured risk assessment determines which measures and countermeasures are recommended for each COA. The OPSEC planner considers the costs associated with these measures and countermeasures when recommending a COA for command approval. The OPSEC planner actions of comparing COAs and recommending them to the commander correspond with the risk management step to develop controls and make risk decisions.

3-10. In risk assessment, the OPSEC planner identifies indicators as potential hazards associated with implementing measures and countermeasures. Indicators can, for purposes of the MDMP, be considered OPSEC-related hazards. The OPSEC planner assesses the risks associated with those hazards before measures (controls) and countermeasures are implemented to mitigate the risk. This risk assessment allows the OPSEC planner to determine whether any identified indicators result in OPSEC vulnerabilities. The OPSEC planner establishes provisional measures and countermeasures to shield OPSEC vulnerabilities and determines the residual risk. Provisional measures and countermeasures, along with adjustments to the initial essential elements of friendly information, represent OPSEC planning guidance, which is disseminated in a warning order after command approval. The residual risk figures aid commanders in deciding how to allocate resources associated with measures and countermeasures and where to accept risk, if necessary.

3-11. During COA approval, the staff recommends a COA to the commander for execution. The recommended COA includes measures and countermeasures identified and tested during preceding MDMP tasks. The OPSEC planner identifies measures and countermeasures that entail significant resource expenditure or risk and requests decisions concerning them. Otherwise, when the commander approves a COA, the measures and countermeasures associated with it are also approved.

3-12. The MDMP concludes with orders production. The OPSEC planner continues the integration process, ensuring that the unit plan or order contains the instructions necessary to prepare, execute, and assess approved measures and countermeasures. The OPSEC planner prepares Appendix 3 (Operations Security) to Annex E (Protection) of the OPORD, specifying approved essential elements of friendly information, measures and countermeasures, coordinating instructions, and tasks for subordinate units. The OPSEC planner monitors and evaluates execution of the recommended measures and countermeasures, determines adjustments and changes to the plan, and disseminates the adjustments to the staff.

This page intentionally left blank.

Chapter 4

Reviews, Assessments, Surveys, and Documentation

4-1. Monitoring and evaluating unit measures and countermeasures continue throughout the OPSEC process and contribute to refining unit OPSEC products. The unit OPSEC planner remains alert for OPSEC indicators that may result in OPSEC vulnerabilities. To provide the feedback needed to adjust and refine unit measures and countermeasures, commanders and OPSEC planners have a number of tools available, such as the OPSEC review, assessment, and survey. These tools serve a dual purpose. They evaluate measures and countermeasures, and they also function as measures themselves, due to their effectiveness in protecting essential elements of friendly information. OPSEC reviews are addressed in most unit standard operating procedures. An OPSEC review is routine but important. OPSEC assessments and surveys are more elaborate and resource intensive. Table 4-1 on page 4-2 describes the differences between OPSEC reviews, assessments, and surveys.

Table 4-1. Operations Security Review, Assessment, and Survey

	OPSEC Review	*OPSEC Assessment*	*OPSEC Survey*
Purpose	Evaluates if official products for public release contain EEFIs.	Determines if current OPSEC measures are sufficient to protect EEFIs.	Reproduces enemy collection capabilities to identify EEFIs vulnerabilities and propose countermeasures.
Scale and Focus	Small to medium. Focused on official information related to military operations and released into the public domain.	Small. Focused on evaluating OPSEC effectiveness.	Large. Focused on analysis of risks associated with an operation either in a command (command survey) or including supporting activities (formal survey).
Frequency	As needed.	Annually.	Every three years or as the operation or commander dictates.
Resources	Internal personnel (for example, OPSEC planner, PA, and other unit staff as needed) for official review. If beyond the local purview (for example, FOIA, intelligence, non-DOD agency), request external, higher headquarters review.	Internal personnel (for example, OPSEC planner, security, PA, communications personnel) carry out the assessment.	Internal and external personnel (for example, communications security monitors, red teams) carry out the survey.
Planning and Design	Minimal. SOP and unit OPSEC plan lists official products to review. Document incidents in the annual unit OPSEC report.	Minimal. May include planning, execution, and analysis phases. Results and recommendations are documented in writing.	Extensive. May include planning, preparation, execution, and post-execution phases. Results are given in a comprehensive report.

DOD	Department of Defense	OPSEC	operations security
EEFI	essential element of friendly information	PA	public affairs
FOIA	Freedom of Information Act	SOP	standard operating procedure

OPERACTIONS SECURITY REVIEW

4-2. An OPSEC review is a documented evaluation of information or visual products intended for public release to ensure protection of essential elements of friendly information. OPSEC reviews are conducted on an as-needed basis. Products that may require an OPSEC review include, but are not limited to, memorandum letters, email messages, articles, speeches, academic papers, videos, briefings, contractual documents, news releases, technical documents, proposals, plans and orders, responses to Freedom of Information Act requests, Privacy Act requests, and other visuals or electronic media. This review is for information related to U.S. Government or military operations and other supporting programs before to release into the public domain. An OPSEC review must be conducted in conjunction with a public affairs review for the release of official unit-related information to the public.

4-3. All staff sections review staff documents and information systems logs to ensure protection of sensitive information. Standard operating procedures should state which documents (for example, news releases) automatically go to the OPSEC planner for review. They should also provide standards for protecting, storing, and handling sensitive information and information systems. When corrective action is necessary, such as an OPSEC assessment or review, the OPSEC planner provides recommendations to the appropriate staff officer.

4-4. In addition to the unit SOP, the OPSEC plan states which products automatically go to the OPSEC planner for a review and which should be handled by a public affairs officer or similarly qualified staff support officer or non-commissioned officer. An OPSEC review may identify additional requirements that include corrective actions, modifications to essential elements of friendly information found in the material under review, or an additional focused intelligence and information security review. When essential elements of friendly information are found and corrective actions are warranted, the OPSEC planner informs the responsible unit staff element and then documents the incident and the subsequent resolution for inclusion in the unit's annual OPSEC report.

4-5. The unit OPSEC planner reviews official, publicly accessible, unit websites to ensure no essential elements of friendly information are posted or contained in other posts. An OPSEC website review is a collaborative responsibility supported by the unit site maintainer, the OPSEC planner, the public affairs officer, and other unit staff as warranted and available. Information unauthorized for release to the public on any website is also unreleasable in any other public forum. Official unit websites must comply with applicable Army and Department of Defense guidance and policies.

4-6. Essential elements of friendly information approved by commanders provide a basis for determining whether information is releasable to the public domain or requires corrective action, such as an OPSEC review. If information requires official review beyond what a local unit OPSEC planner can provide (for example, Freedom of Information Act, intelligence, foreign disclosure, information security, or non-Department of Defense agency information), the OPSEC planner forwards the matter with a written request for such review to higher headquarters for resolution.

OPERATIONS SECURITY ASSESSMENT

4-7. An OPSEC assessment is an evaluative process to determine if sufficient measures and countermeasures are in place to protect essential elements of friendly information. OPSEC assessments monitor an operation to determine a unit's overall OPSEC posture and evaluate compliance of subordinate organizations with Appendix 3 (Operations Security) to Annex E (Protection) of the OPORD (see FM 6-0 for further discussion of OPORD annexes and appendixes). An OPSEC assessment team is led by the OPSEC planner, but can include other members of the unit staff. Results are submitted to the commander.

4-8. The OPSEC planner annually assesses the effectiveness of the unit OPSEC program, and at a minimum, assesses the status of the following:

- Unit personnel's knowledge of essential elements of friendly information.
- Unit personnel's knowledge of the collection threat.
- Measures and countermeasures in place to protect identified essential elements of friendly information.
- Status of OPSEC training.

4-9. The OPSEC planner leads an overarching OPSEC assessment of assigned subordinate units using the unit-published OPSEC guidance to determine if each subordinate unit is implementing higher headquarters directed-and their own-OPSEC policies and procedures. The unit OPSEC planner submits written results and recommendations to the assessed subordinate unit commander or the commander that directed the assessment. At a minimum, the following is assessed:

- Identification of essential elements of friendly information.
- Unit personnel's knowledge of essential elements of friendly information.
- Unit personnel's knowledge of the collection threat.
- Measures and countermeasures in place to protect identified essential elements of friendly information.
- Status of OPSEC training.
- Application of a formal OPSEC checklist based on restrictions in existing laws, statutes, regulations and policy, including requirements applicable only to the assessed unit.

4-10. Higher headquarters develops and publishes an OPSEC checklist or checklists, as warranted, and may include these as part of the command inspection program. The commander performing the inspection determines the areas of interest and the scope of the inspection. The inspection team reports its findings to higher headquarters.

OPERATIONS SECURITY SURVEY

4-11. The objective of an OPSEC survey is to identify OPSEC vulnerabilities in unit operations or activities that an enemy could exploit to degrade unit effectiveness. The survey helps the commander evaluate measures and countermeasures and take further action to protect essential elements of friendly information. For the OPSEC survey, a team of experts applies OPSEC methodology to analyze specific unit activities in detail, considering among various factors the known collection capabilities of potential enemies. It focuses on the unit's ability to adequately protect essential elements of friendly information from enemy intelligence exploitation during planning, preparation, execution, and post-execution phases of an operation.

4-12. The OPSEC survey attempts to reproduce the intelligence image that an operation projects. The survey differs from an enemy's collection effort, since it occurs within a limited timeframe, and normally does not use covert means. From that image, the survey identifies exploitable information sources. It verifies the existence of indicators by examining all of a unit's functions during planning, coordination, and execution of the operation. The examination traces the chronological flow of information from start to finish for each function.

4-13. Unit OPSEC surveys vary according to the nature of the information, the enemy collection capability, and the environment. In combat, surveys identify weaknesses that can endanger ongoing and impending combat operations. In peacetime, surveys help to correct weaknesses that disclose information useful to enemies in future conflict. A survey will not serve as an inspection of the effectiveness of a unit's security programs or adherence to security directives. Each survey is unique, as it reflects the unit operation or activity it analyzes.

4-14. An OPSEC survey can be either a command survey or a formal survey. A command survey concentrates on events that happen solely in the command. It uses the personnel resources of the command to conduct the survey. A formal survey includes supporting activities beyond the control of the operation that is the focus of the survey (it crosses organizational lines with prior coordination). The survey team includes members from both inside and outside the surveyed unit. A formal survey is initiated by a letter or message that states the subject, team members, and dates of the survey and can also list units, activities, and locations.

4-15. Whether categorized as a command or formal survey, the survey team encourages open dialogue and does not attribute data to their source. An accurate survey depends on cooperation by all unit personnel. The OPSEC survey team does not submit a report to the surveyed unit's higher headquarters. As appropriate, the survey team can provide lessons learned without reference to specific units or individuals. A report can be provided to the requesting commander. Surveys are typically scheduled every three years or when requested by the commander.

4-16. OPSEC surveys are personnel, resource, and time intensive, which is why they are conducted only every three years for tactical units. In some cases, higher headquarters requires a unit to conduct an out-of-cycle survey (a survey in addition to the normal survey cycle). Extremely sensitive unit operations where the slightest compromise will result in mission failure or extreme damage to national security are rare examples of where out-of-cycle OPSEC surveys are warranted.

OPERATIONS SECURITY DOCUMENTATION

4-17. The purpose of OPSEC documentation is to ensure that units are aware of, and understand, unit essential elements of friendly information and measures and countermeasures. By understanding the measures and countermeasures, units are encouraged to practice them on a consistent and continuous basis. OPSEC documentation normally includes unit OPSEC policy, threat analysis, essential elements of friendly information indicators, a list of potential vulnerabilities and the associated risks, and measures and countermeasures to mitigate the risks. Documentation can take the form of an SOP, plan, or other procedural format.

4-18. Essential elements of friendly information are a key aspect of unit OPSEC documentation. Many units opt to limit the number of essential elements of friendly information to fewer than ten for simplicity; however, commanders ultimately determine the number of essential elements of friendly information. Dissemination and communication of essential elements of friendly information to the lowest organizational level and to all personnel is critical.

4-19. OPSEC documentation is reviewed at least annually to ensure that changes in mission, threats, essential elements of friendly information, or measures and countermeasures are updated into unit SOPs and plans in a timely manner. A memorandum is typically attached to OPSEC documents more than a year old to verify that unit SOPs and plans have been reviewed and updated annually. Additional coordination is performed with other security programs, such as units' information security, information assurance, physical security, force protection, and anti-terrorism. This ensures that units' security programs work collaboratively to support unit operations and do not provide conflicting guidance.

4-20. The unit intelligence staff provides written regional threat assessments in support of OPSEC. Written threat information provides additional clarity and purpose for many of the measures and countermeasures approved for implementation. Threat assessments are updated as necessary to reflect units' current situation and environment.

4-21. Lastly, in the case of an OPSEC compromise that involves essential elements of friendly information made available through open sources, the compromise and its public domain location should be documented and the incident forwarded for further review and resolution to higher headquarters using intragovernmental or authorized official communications. Disclosing the information publically only serves to unnecessarily subject the information to further exposure and potential dissemination. Personnel should not respond to queries to deny or confirm the validity of essential elements of friendly information that have been compromised or released to the public. The appropriate action is to notify the unit OPSEC planner or security manager of suspected instances of OPSEC compromises.

This page intentionally left blank.

Appendix A

Appendix 3 (Operations Security) to Annex E (Protection): Tips and Recommendations

A-1. OPSEC is a responsibility of the protection warfighting function and, for Army units, is documented in Appendix 3 (OPSEC) to Annex E (Protection) of an operation order (OPORD)(see FM 6-0 for further discussion). This Appendix contains helpful tips for developing an OPSEC appendix. This appendix also provides an example of a completed OPSEC appendix to support a notional OPORD.

A-2. *Paragraph 1, Situation.* This paragraph contains information affecting measures and countermeasures not otherwise included in paragraph 1 of the OPORD.

- Area of interest—describe the information environment as it relates to OPSEC.
- Terrain—address those aspects of terrain that impact unit OPSEC or that require specific actions because of the terrain.
- Weather—address those aspects that affect the performance of OPSEC tasks or the systems employed by the unit to accomplish OPSEC tasks.
- Enemy forces—describe enemy forces in detail. List: (1) known and template-derived locations and activities of threat sensors and (2) information and intelligence gathering systems that have the capability to collect information on unit capabilities, activities, limitations, and intent. Discuss enemy capabilities and systems in terms of strengths and weaknesses.
- Friendly forces—provide an overview of the higher headquarters' plan and the role OPSEC plays through the implementation of measures and countermeasures to control and protect essential elements of friendly information.
- Interagency, intergovernmental, and nongovernmental organizations—discuss the impact these organizations have on unit OPSEC within the area of operations. Identify and describe the organizations in the area of operations that may impact the conduct of unit OPSEC or implementation of OPSEC tactics. Identify measures and constraints in place when communicating with these organizations to ensure OPSEC is maintained. Identify sensors and conduits in these organizations that may provide essential elements of friendly information to an enemy force.
- Civil considerations—describe critical aspects of the civil situation that impact OPSEC. Consider these factors and how they impact unit OPSEC activities and objectives:
  - News media collection and dissemination. Describe media activities that have access to, gather, and report on unit observables of interest to enemy decision makers through known or suspected conduits in the unit's area of operations.
  - Local population collection and dissemination. Describe local citizen activities that may potentially allow gathering and reporting of unit observables of interest to enemy forces through known or suspected conduits in the unit's area of operations.
  - Home station friends and family. Describe home station friends' and families' access to unit command information, public affairs information, family readiness group information, social media interaction with unit Soldiers, sensitive observables, and other essential elements of friendly information that may be available to enemy forces through known or suspected conduits in the unit's area of operations.
- *Attachments and detachments*—list and describe units that conduct information related capabilities only as necessary to clarify task organization. Examples include tactical military information teams, mobile public affairs detachments, and visual information teams.

A-3. *Paragraph 2, Mission.* Summarize the mission of the OPSEC support detailed in the base order.

A-4. *Paragraph 3, Execution.* Summarize the scheme of support, assessment, tasks to subordinate units, and coordinating instructions as they relate to the unit OPSEC support strategy.

- Scheme of support—describe how OPSEC applies to all aspects of unit operations. The unit conducts OPSEC to protect essential elements of friendly information from threat exploitation and to support the commander's intent and concept of operations. Describe the general concept and any additional measures and countermeasures with other staff and command elements. Synchronize the unit's measures and countermeasures with adjacent units.
  - Identify actions that can be observed by enemy intelligence and surveillance systems during each phase of the operation.
  - Determine indicators observable by enemy intelligence systems that, if acquired, could be interpreted or pieced together to derive essential elements of friendly information in time to be useful to the enemy.
  - Describe how to execute measures and countermeasures that eliminate, or reduce to acceptable levels, the vulnerabilities of friendly actions.
- Assessments—describe the priorities for assessment, identify measures of performance and effectiveness, determine indicators of measures and countermeasures, and evaluate enemy collection capabilities to identify and act upon command essential elements of friendly information.
- Tasks to subordinate units—list OPSEC tasks assigned to subordinate units not contained in the base order.
- Coordinating instructions—summarize coordinating instructions involving implementation of unit measures and countermeasures to subordinate units not otherwise covered in the base order.
  - List only OPSEC instructions applicable to two or more subordinate units not covered in the base order.
  - Identify required coordination with public affairs.
  - Identify the guidance on declassification and public release of OPSEC-related information.
  - Identify reporting requirements for OPSEC violations.

A-5. *Paragraph 4, Sustainment.* Identify priorities of sustainment for OPSEC tasks and specify additional instructions as required.

A-6. *Paragraph 5, Command and signal*. For each aspect of command, control, and signal, summarize the intent, key information, and operational requirement. For command, state the location of key OPSEC relevant personnel. For control, state the OPSEC liaison requirements not covered in the base order. For signal, address any OPSEC-specific communication requirements or reports.

Appendix 3 (Operations Security) to Annex E (Protection) Example

Copy XX of XX copies
52 ID HQ
ATK PSN GRIZZLY, ATROPIA
DTG DDXXXX(**D**)MMM19 (W+55)

APPENDIX 3 (OPERATIONS SECURITY) TO ANNEX E (PROTECTION) TO OPORD 3995-19 (OPERATION ITEM SHIVA) – 52 ID

References:

a. AR 530-1, Operations Security, September 2014
b. DODD 5205.02E, DOD Operations Security (OPSEC) Program, June 2012.
c. ADP 3-37, Protection, December 2018.
d. FM 3-13, Information Operations, December 2016
e. ATP 3-37.2, Antiterrorism, June 2014.

Time Zone Used Throughout the OPORD: DELTA.

1. Situation.

a. Enemy:

(1) Capabilities (Strengths).

(a) Reconnaissance Vehicles. Enemy forces conduct continuous and pervasive reconnaissance activity throughout the battlefield before and during all phases of military operations. To accomplish this, ground forces employ a mix of vehicles that vary based on types of threat and mobility requirements. The variety of reconnaissance vehicles currently ranges from older systems ill-suited for modern requirements to survivable, mobile, and lethal systems equipped with complex sensor arrays and communications suites. Some of the vehicles must act as independent reconnaissance patrols, combat reconnaissance patrols, security patrols, and combat outposts against high-threat forces. Many reconnaissance missions will be executed by maneuver units using organic vehicles such as armored personnel carriers, tanks, infantry fighting vehicles, and combat support vehicles.

(b) Sensors for Tactical Ground Forces. Reconnaissance units use a mix of high and low technologies. Enemy forces may perform tactical reconnaissance using troops with specially designed reconnaissance assets as well as infantry Soldiers from maneuver units.

1. Improved Day Sights. Enemy forces will have a mix of older and newer infantry weapons with varying upgrades of sight systems. Most have the original day sights which came from the factory. Most improved sights are used for observation and surveillance by reconnaissance elements. Many improvements have been made to the quality, durability, and performance of sight systems:

a. Plastics, composites, and graphite materials for lightweight weather-resistant housings.

b. Improved optics and graticules for wider fields of view, magnification where needed, and a variety of sight pictures.

c. Electro-optics to help manipulate the sight picture, for example, zooming in and out for specific weapon needs.

d. Compact ballistic computers that can be incorporated into sight systems.

2. Night Sights. In recent years, enemy forces have prioritized acquisition of passive night-fighting technologies to eliminate that vulnerability. They employ thermal imaging cameras, which see light in the 3-5 micrometer or 8-12 micrometer band from heat (temperature differential) as a digital image, then convert it to a microchannel plate in the viewer. Thermal imaging systems have seen many improvements in processing and display technologies. The three greatest limitations of thermal imaging for weapon sights have been weight, size, and cost. Vulnerability mitigation to superior night systems can be achieved by using cover and concealment, exploiting civilian illumination, and using other reconnaissance systems such as hand-held night viewers, radars, unattended ground sensors (for detection and location), infrared illumination rounds, and infrared markers, night vision goggles, and laser aimers or pointers to direct fires.

(c) Radars. Battlefield surveillance radar mounts include tripods, carriage, weapon and vehicle mounts, and aerial platforms, even trees. Technologies such as miniaturization, millimeter-wave, improved power supplies, and links to laptop computers offer new radar applications, such as the day and night future combat system. Compact radars offer man-portable carry and attachment to weapons, such as automatic grenade launchers for fire direction. Slightly larger systems offer a two-man radar system with a 24-kilometer operating range and portability in carry packs. Tripod-mounted radars can link to digital nets and be quickly emplaced or displaced.

(d) Air Space.

1. Rotary Wing.

a. Donovian Attack Helicopter Mi-24K or HIND G-2. A photo-reconnaissance and artillery fire direction variant that is equipped with avionics, sensors, and advanced optics.

b. Donovian Medium Multirole Helicopter Mi-2URP (HOPLITE). An armed reconnaissance variant that employs 57-millimeter unguided rockets equipped with a pilot sighted cannon that is also used for reconnaissance purposes.

2. Fixed Wing. Some fixed-wing aircraft are modified from fighter or interceptor, strike, ground attack, and bombers to reconnaissance variants, which are extremely effective in designating targets and collecting enemy intelligence.

a. RF-5E Tigereye. Photo-reconnaissance version with a modified nose that accepts a variety of camera-carrying pallets and mounts an oblique-frame camera. Equipped with an austere avionics package including a radar gun sight, a pulse Doppler radar, communications and navigation equipment, lead-computing optical sight, central air data computer, and forward-looking infrared.

b. Donovian Interceptor Aircraft MiG-25-R or FOXBAT-B. All remaining in service are strictly reconnaissance aircraft. They are equipped with avionics, sensors, and optics. An infrared search and track sensor pod is located under the front fuselage, and an infrared sensor is located under the nose.

c. Donovian Transport Aircraft Il-20 or COOT A. Unarmed strategic electronic information reconnaissance and surveillance aircraft. The airframe is essentially the same as the Il-18D, but a cylinder containing a possible side-looking airborne radar is mounted under the fuselage forward of the wing. Smaller containers on the forward sides of the fuselage house possible cameras and sensors. Many small antennas are located under the fuselage.

3. Unmanned Aircraft. Technologies include remotely-launched sensor munitions with still cameras or video-cameras, which sense and emit while in their trajectory.

a. Donovian Unmanned Aircraft System Tu-143. The Tu-143 can operate to a reconnaissance depth of 150 kilometers and is preprogrammed before each mission. Survivability or countermeasures: radar altimeter permits a flight profile with up to four altitude changes. Equipped with PA-1 panoramic camera, Chibis-B low-light-level TV, and radiation detection equipment. Camera data must be processed upon return. Infrared linescan (with side scan) and radiation detection equipment can be used.

b. Mini-Unmanned Aircraft System Skylark IV. Equipped with day optics, such as a gimballed gyro-stabilized daylight charge-coupled device camera with electro-optical auto-tracker, which aids in tracking moving vehicles. Also equipped with a thermal camera for night operations.

(2) Capabilities (Weaknesses).

(a) Reconnaissance Vehicles. Tough utility vehicles can move undetected by enemy forces; however, most tough utility vehicle chassis are poorly suited to the stresses of structural and weight increases with true all-over armor protection or even for real protection against the most likely weapons. Also, wheels are generally vulnerable to all weapons. Added armor on tough utility vehicles remains a compromise at best. Vehicles which are equipped to haul added weight or stress lack the ability to move around undetected.

(b) Sensors for Tactical Ground Forces. Thermal imaging has several weaknesses—it does not convert images into shapes; temperature changes alter shapes and render objects invisible; and lack of heat among selected materials—meaning that thermal imaging may not see objects in the foreground or background, and it is a much more expensive technology.

(c) Radars. One disadvantage of radars is that they actively emit, thus U.S. forces electronic warfare and other systems can detect the radar emissions and attacked. Enemy forces use Squire Radar, which has a low probability of interception due to its extremely low peak power. Other low probability of intercept features include phased arrays with lower power levels for detectors; reduced side lobes; and operating frequencies outside of most radar intercept system bandwidths.

(d) Air Space. One major disadvantage that enemy forces have with employing fixed- and rotary-wing aircraft is the lack of ability to "fight" at night. Most are equipped with night vision goggles—but only to fly at night— not to conduct night operations. Unmanned aircraft systems have a disadvantage due to their lack of survivability and, in most cases, range of flight.

b. Friendly. Operations security (OPSEC) planning is severely challenged by telecommunications products—computers, cell phones, laptops, and global positioning systems—available to the command. Measures must be taken to control the use of these and other unsecure communications means.

c. Civil Considerations. The enemy has been known to influence the local population to report any intelligence on U.S. or multinational force actions or locations. U.S. forces are to remain vigilant when conducting operations in the civilian population.

2. Mission. Commanders at all levels will integrate measures and countermeasures to protect their command's essential elements of friendly information in every phase of all operations. These measures will also be coordinated and synchronized with security programs such as information security, information assurance, physical security, and force protection.

3. Execution.

a. Scheme of Support. OPSEC is every Soldier's responsibility. Failure to properly implement measures and countermeasures can result in serious injury or death to our personnel; damage to weapons systems, equipment, and facilities; loss of sensitive technologies; and mission failure. OPSEC must be fully integrated into the conduct of all operations and supporting activities. The command and its subordinate elements shall use the following process: identify essential elements of friendly information, analyze threats, evaluate vulnerabilities, assess risk, and recommend measures and countermeasures.

(1) Identify essential elements of friendly information. Essential elements of friendly information comprise specific facts about friendly capabilities, activities, limitations (including vulnerabilities), and intentions needed by the enemy to plan and act effectively so as to degrade friendly mission accomplishment. The commander's essential elements of friendly information requirements are as follows:

(a) Time and destination of any logistical movements.

(b) Location of division-forward arming and refueling points, logistical support areas, and headquarters.

(c) Time and location of one unit's forward passage of lines through another unit.

(d) Location of an infantry brigade combat team before air assault operations.

(e) Any information regarding timing and direction of an infantry brigade combat team's air assault.

(f) Combat strength of ground maneuver brigade combat teams before Phase II.

(2) Analyze Threats. Enemy collection activities target actions and open-source information to obtain and exploit indicators that will negatively impact the mission. Each subordinate OPSEC planner, in coordination with the intelligence staff, examines each part of the operation to find actions or information that provide indicators in the following areas:

(a) Administrative

(b) Operations, Plans, and Training

(c) Communications

(d) Intelligence

(e) Logistics

(f) Engineering

(g) Medical

(3) Evaluate Vulnerabilities and Assess Risk. OPSEC planners and staff identify each vulnerability and draft provisional measures and countermeasures addressing those vulnerabilities. The most desirable measures and countermeasures provide needed protection at the least cost to operational effectiveness and efficiency. Measures are identified as follows:

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

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

(c) Operate to minimize reflective surfaces that units and weapons systems present to radar and sonar.

(d) Randomize indicators such as convoy routes, departure times, and speeds.

(e) Do not repeatedly use the same landing zone or pick-up point.

(f) Use low probability of intercept techniques; radio communications emission controls; traffic flow security; ultrahigh frequency relays via aircraft; burst transmission technologies; and secure phones, landlines, and couriers. Limit use of high-frequency radios and directional super-high-frequency transponders.

(g) Maintain noise discipline, operate at reduced power, proceed at slow speeds, and turn off selected equipment.

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

(i) Control trash dumping. Destroy (for example, burn or shred) paper, including unclassified information, to prevent the inadvertent disposal of classified and sensitive information.

(j) Maximize use of security screening of local national hires and minimize their access and observation opportunities.

(k) Perform random internal unannounced identity and security inspections.

(4) Recommend Measures and Countermeasures. The OPSEC planner will recommend and monitor implementation of measures and countermeasures, evaluating them regarding their probability of success. The OPSEC planner adjusts measures and countermeasures, if necessary, based on this assessment. The OPSEC planner coordinates monitoring of measures and countermeasures with the staff officer and counterintelligence staffs to ensure monitoring receives the appropriate priority.

b. Coordinating Instructions.

(1) Do not publicly disseminate or publish photographs displaying critical or sensitive information. Examples include, but are not limited to, improvised explosive device strikes, battle scenes, casualties, destroyed or damaged equipment, personnel killed in action—both friendly and threat—and the protective measures of military facilities.

(2) Process, store, or transmit classified information no higher than the approved accreditation level of a DOD computer system, including all related equipment, networks, network devices (including internet access), and removable media devices.

(3) Destroy (burn or shred) unneeded critical and sensitive information to prevent the inadvertent disclosure and reconstruction of this material.

(4) The operations staff officer and the information operations staff officer provide input for the essential elements of friendly information, which includes what they obtain from the intelligence and signal staff officers. Essential elements of friendly information and the vulnerability assessment form the basis for planning defensive information operations. The information operations staff officer establishes one or more information operations objectives that focus on protecting critical assets or centers of gravity.

(5) Eliminate indicators or the vulnerability of actions to exploitation by adversary information collection systems. Select what actions to undertake, decide whether to execute actions, and determine the "who, when, where, and how" for actions necessary to accomplish tasks.

(6) Ongoing measures and countermeasures to ensure an effective OPSEC posture include, but are not limited to the following: counterreconnaissance, physical security, command information, communications security, network security, subversion and espionage prevention, camouflage, active patrolling, electronic and physical masking, and information control. As warranted, use diversions, camouflage, concealment, jamming, threats, police powers, and force against adversary information gathering and processing capabilities. Implement at a minimum the following protective measures:

(a) Implement special access requirements with limited compartmentalized access and entry on a need to know basis.

(b) Use standard cryptologic systems and devices. Cell phones and the nonsecure internet protocol router network, commonly known as NIPRNET, are unprotected communication methods.

(c) Develop essential elements of friendly information and submit to the OPSEC planner.

(d) Establish OPSEC policy and procedures; prepare OPSEC estimates, plans, and annexes; review all plans and orders to ensure adherence to OPSEC policies and procedures; assist in developing friendly force profiles; evaluate operational risks; select measures and countermeasures; and direct OPSEC estimates.

(e) Perform counterintelligence functions and coordinate the collection and processing of intelligence to support the OPSEC program.

(f) Support division risk analysis and recommend measures, countermeasures, and evaluation requirements.

(7) Prevent accurate interpretations of indicators during adversary analysis of collected materials.

(8) Coordinate measures and countermeasures with Public Affairs and Civil Affairs to support public information campaigns and deception efforts.

(a) The assistant chief of staff, operations, is the approval authority for specific command-wide measures and countermeasures, as well as declassification and public release of OPSEC-related information.

(b) Report all suspected compromises of essential elements of friendly information to the OPSEC planner.

(c) All subversion and espionage investigations and countersubversion and espionage operations will be performed by the counterintelligence element.

(9) Unit elements will:

(a) Know what their organization considers to be essential elements of friendly information; where they are located; who is responsible for them; how to protect them; and why they need to be protected.

(b) Protect from disclosure any essential elements of friendly information to which they have personal access.

(c) Prevent disclosure of essential elements of friendly information in any public domain including, but not limited to, the internet, open-source publications, and both traditional and social media.

(10) The OPSEC planner and staff assess the risks posed by OPSEC vulnerabilities throughout all phases of the operation.

(11) Staffs present to the commander for approval a prioritized list of essential elements of friendly information requiring protection. The commander approves, by phase, a prioritized list of essential elements of friendly information to be protected based on the resources available. The list of essential elements of friendly information will be refined and, where necessary, modified based on changing mission requirements, shifting priorities, and resource availability. Staffs should consider, but not be limited to, the following unit-related information for inclusion as essential elements of friendly information:

(a) All communications in reference to operational planning and execution.

(b) Designation and locations of participating units.

(c) Alert states or status.

(d) Target lists and routes.

(e) Requests for information collection resources.

(f) Gaps in information collection coverage.

(g) Requests for additional tankers and airlift support for operations.

(h) Flying schedules.

(i) Timing of air (including fixed and rotary) operations.

(j) Re-supply items and schedule.

(k) Intended military information support operations objectives.

(l) Capabilities, missions, and areas of operations of special operations forces.

(m) Weapons used and weapons shortfalls.

(n) Movements and itineraries.

(o) Radio frequencies.

(p) Identification of personnel in key positions.

(q) Identification of force protection measures and shortfalls.

(r) Troop movements (unless to support deception activities).

(s) Own force passwords, pro-words, and code words linked to their actual meaning.

4. Sustainment. Refer to Annex F (Sustainment) as required.

5. Command and Signal.

a. Command. Refer to Annex E (Protection) as required.

b. Control.

(1) Command Posts. Refer to Annex E (Protection) as required.

(2) Reports. As per SOP.

(a) OPSEC assessments will be performed by the OPSEC planner and assistant chief of staff, operations protection cell chief, throughout ongoing operations.

(b) OPSEC compromises will be IMMEDIATELY reported through command channels.

c. Signal. Refer to Annex E (Protection) as required.

ACKNOWLEDGE:

YOUNGBLOOD
COL

OFFICIAL:
SMITH-JONES
G-3

This page intentionally left blank.

Glossary

The glossary lists acronyms and terms with Army or joint definitions. Where Army and joint definitions differ, (Army) precedes the definition. The proponent publication for terms is listed in parentheses after the definition.

SECTION I – ACRONYMS AND ABBREVIATIONS

ADP	Army doctrine publication
ADRP	Army doctrine reference publication
AR	Army regulation
ATP	Army techniques publication
CI	critical information
COA	course of action
DA	Department of the Army
DD	Directives Division
DOD	Department of Defense
DODD	Department of Defense directive
DODI	Department of Defense instruction
FM	field manual
G-2	assistant chief of staff, intelligence
G-3	assistant chief of staff, operations
JP	joint publication
MDMP	military decisionmaking process
OPORD	operation order
OPSEC	operations security
S-2	battalion or brigade intelligence staff officer
S-3	battalion or brigade operations staff officer
SOF	special operations forces
SOP	standard operating procedure

SECTION II – TERMS

adversary

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

civil considerations

The influence of manmade infrastructure, civilian institutions, and activities of the civilian leaders, populations, and organizations within an area of operations on the conduct of military operations. (ADRP 5-0)

controlled unclassified information

Unclassified information to which access or distribution limitations have been applied according to national laws, policies, and regulations of the U.S. Government. It includes U.S. information that is determined to be exempt from public disclosure according to DODD 5230.25, DODD 5400.07, AR 25–55, AR 530–1, and so on, or that is subject to export controls according to the International Traffic in Arms Regulations or the Export Administration Regulations. (AR 530-1)

counterintelligence

Information gathered and activities conducted to identify, deceive, exploit, disrupt, or protect against espionage, other intelligence activities, sabotage, or assassinations conducted for or on behalf of foreign powers, organizations or persons or their agents, or international terrorist organizations or activities. Also called CI. See also counterespionage; security. (JP 2-01.2)

countermeasures

That form of military science that, by the employment of devices and/or techniques, has as its objective the impairment of the operational effectiveness of enemy activity. (JP 3-13.1)

critical information

Specific facts about friendly intentions, capabiliteis, and activities needed by adversaries for them to plan and act effectively so as to guarantee failure or unacceptable consequences for friendly mission accomplishment. (JP 2-0)

essential element of friendly information

(Army) A critical aspect of a friendly operation that, if known by the enemy, would subsequently compromise, lead to failure, or limit success of the operation and therefore should be protected from enemy detection. (ADRP 5-0)

force protection

Preventive measures taken to mitigate hostile actions against Department of Defense personnel (to include family members), resources, facilities, and critical information. Also called FP. (JP 3-0)

high-risk personnel

Personnel who, by their grade, assignment, symbolic value, or relative isolation, are likely to be attractive or accessible terrorist targets. Also called HRP. See also antiterrorism. (JP 3-07.2)

indicator

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)

information operations

The integrated employment, during military operations, of information-related capabilities in concert with other lines of operation to influence, disrupt, corrupt, or usurp the decision-making of adversaries and potential adversaries while protecting our own. Also called IO. See also electronic warfare; military deception; military information support operations; operations security. (JP 3-13)

military decisionmaking process

An iterative planning methodology to understand the situation and mission, develop a course of action, and produce an operation plan or order. (ADP 5-0)

operations security

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

operations security assessment

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

operations security compromise

The disclosure of critical information or sensitive information which has been identified by the command and any higher headquarters that jeopardizes the unit's ability to execute its mission or to adequately protect its personnel and/or equipment. (AR 530-1)

operations security planning guidance

Guidance that defines the critical information requiring protection from the adversary and outlines provisional measures to ensure secrecy. (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 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 3-13.3)

retrograde

A defensive task that involves organized movement away from the enemy. (ADP 3-90)

sensitive

An agency, installation, person, position, document, material, or activity requiring special protection from disclosure that could cause embarrassment, compromise, or threat to the security of the sponsoring power. (JP 2-01)

threat

Any combination of actors, entities, or forces that have the capability and intent to harm United States forces, United States national interests, or the homeland. (ADRP 3-0)

This page intentionally left blank.

References

All URLs accessed on 3 June 2019.

REQUIRED PUBLICATIONS

These documents must be available to intended users of this publication.

DOD Dictionary of Military and Associated Terms. May 2019.

ADP 1-02. *Terms and Military Symbols.* 14 August 2018

RELATED PUBLICATIONS

These publications are referenced in this publication.

DEPARTMENT OF DEFENSE PUBLICATIONS

DOD Issuances are available online at: https://www.esd.whs.mil/DD/DoD-Issuances/.

FOUO DOD instructions are available online through the Joint Electronic Library Plus at: https://jdeis.js.mil/jdeis/index.jsp.

DODD 5205.02E. *DOD Operations Security (OPSEC) Program.* 20 June 2012.

DODD 5230.25. *Withholding of Unclassified Technical Data from Public Disclosure.* 6 November 1984.

DODD 5400.07. *DOD Freedom of Information Act (FOIA) Program.* 5 April 2019.

DODI O-2000.22. *Designation and Physical Protection of DOD High-Risk Personnel.* 19 June 2014. (For Official Use Only)

JOINT PUBLICATIONS

Most joint publications are available online at: https://www.jcs.mil/doctrine/.

JP 2-0. *Joint Intelligence*. 22 October 2013.

JP 2-01. *Joint and National Intelligence Support to Military Operations.* 5 July 2017.

JP 2-01.2. *Counterintelligence and Human Intelligence in Joint Operations (U).* 6 April 2016. (This classified publication is available on the SIPRNET. Contact the preparing agency of this publication for access instructions.)

JP 3-0. *Joint Operations.* 17 January 2017.

JP 3-07.2. *Antiterrorism.* 14 March 2014.

JP 3-13. *Information Operations.* 27 November 2012.

JP 3-13.1. *Electronic Warfare.* 8 February 2012.

JP 3-13.3. *Operations Security.* 6 January 2016.

ARMY PUBLICATIONS

Army doctrinal publications are available on the Army Publishing Directorate website: https://armypubs.army.mil/.

ADP 3-37. *Protection*. 11 December 2018.

ADP 3-90. *Offense and Defense.* 13 August 2018.

ADP 5-0. *The Operations Process.* 17 May 2012.

ADRP 3-0. *Operations.* 6 October 2017.

ADRP 5-0. *The Operations Process.* 17 May 2012.

ADRP 6-0. *Mission Command.* 17 May 2012.

AR 25-55. *The Department of the Army Freedom of Information Act Program.* 1 November 1997.

AR 530-1. *Operations Security.* 26 September 2014.

ATP 3-37.2. *Antiterrorism.* 3 June 2014.

ATP 5-19. *Risk Management.* 14 April 2014.

FM 3-13. *Information Operations.* 6 December 2016.

FM 3-39. *Military Police Operations.* 9 April 2019.

FM 3-90-1. *Offense and Defense,* Volume 1. 22 March 2013.

FM 6-0. *Commander and Staff Organization and Operations.* 5 May 2014.

FM 27-10. *The Law of Land Warfare.* 18 July 1956.

RECOMMENDED READINGS

This section contains no entries.

PRESCRIBED FORMS

This section contains no entries.

REFERENCED FORMS

DA forms are available on the Army Publishing Directorate website: https://armypubs.army.mil.

DD forms are available through the Joint Electronic Library Plus website: https://jdeis.js.mil/jdeis/index.jsp.

DA Form 2028. *Recommended Changes to Publications and Blank Forms*.

DD Form 2977. *Deliberate Risk Assessment Worksheet*.

Index

Entries are by paragraph number.

This page intentionally left blank.

ATP 3-13.3
16 July 2019

By Order of the Secretary of the Army:

MARK A. MILLEY
General, United States Army
Chief of Staff

Official:

Kathleen S. Miller

KATHLEEN S. MILLER
Administrative Assistant
to the Secretary of the Army
1917601

DISTRIBUTION:
Distributed in electronic media only(EMO).

PIN: 205361-000