

Training and Evaluation Outline Report

Task Number: 71-8-6111

Task Title: Plan Operations Security (Battalion - Corps)

Supporting Reference(s):

Step Number	Reference ID	Reference Name	Required	Primary
	ADP 3-0	Unified Land Operations	Yes	No
	FM 3-13	Inform and Influence Activities	Yes	Yes
	FM 5-0	(Superseded 17 May 2012 by ADP 5-0) THE OPERATIONS PROCESS	Yes	No
	FM 6-0	(Superseded by ADP 6-0 17 May 2012) MISSION COMMAND	Yes	No

Condition: The command has received an operations plan, warning, operations, or fragmentary order from higher headquarters and is exercising mission command. The commander has issued planning guidance for operations security in order to execute measures that eliminate or reduce the acceptable level and vulnerabilities of friendly actions to adversary exploitation. The command has established communications with subordinate and adjacent units, and higher headquarters. The mission command system is operational and processing information in accordance with standard operating procedures. Some iterations of this task should be performed in MOPP.

Standard: The staff conducts operations security measures in the decision making process by application of moderate protection of essential elements of friendly information, denying adversaries collection and exploitation of information about friendly capabilities and intentions, and by identifying, controlling, and protecting indicators associated with planning and conducting operations.

Note: Task steps and performance measures may not apply to every unit or echelon. Prior to evaluation, coordination should be made between evaluator and the evaluated units' higher headquarters to determine the performance measures that may not be evaluated.

Special Equipment: None

Safety Level: Low

Task Statements

Cue: None

DANGER

Leaders have an inherent responsibility to conduct Composite Risk Management to ensure the safety of all Soldiers and promote mission accomplishment.

WARNING

Composite Risk Management is the Army's primary decision-making process to identify hazards, reduce risk, and prevent both accidental and tactical loss. All soldiers have the responsibility to learn and understand the risks associated with this task.

CAUTION

Identifying hazards and controlling risks across the full spectrum of Army functions, operations, and activities is the responsibility of all Soldiers.

Remarks:

Notes: Task content last updated: 14 Feb 2013.

TASK STEPS

1. The staff led by the operations section and operations security (OPSEC) officer conducts the five actions of the OPSEC process.

Note: Action one

a. Action 1- Identify essential elements of friendly information (EEFI) from:

- (1) The commander's guidance.
- (2) The information operations (IO) estimate.
- (3) The OPSEC estimate.
- (4) The intelligence estimate.
- (5) The multi discipline counterintelligence estimate.
- (6) The higher headquarters security classification guide for the operation.
- (7) Laws and executive orders that require protection of unclassified controlled information.

Note: Action two

b. Action 2- Conduct analysis of adversaries:

- (1) The intent and capabilities of the adversaries to act against the planned operation.
- (2) The probable adversary objectives.
- (3) The likely adversary actions against friendly operations.
- (4) The information the adversaries already know.
- (5) The collection capabilities the adversaries possess or have access to by financial arrangement or shared ideologies, or coordinated coalitions/ alliances.

(6) The OPSEC indicators that can be faked to deceive adversaries.

Note: Action three

c. Action 3- Analyze vulnerabilities.

- (1) Identify OPSEC indicators.
- (2) Select at least one OPSEC measure for each vulnerability (personnel, physical, cryptographic, document, special access, and automated information systems).

(3) Identify possible OPSEC measures for each vulnerability.

Note: Action four

d. Action 4- Assess risk.

- (1) Conduct a risk assessment for each OPSEC vulnerability.

(2) Select one or more OPSEC measure for each OPSEC vulnerability.

(3) Determine residual risk for each OPSEC vulnerability.

(4) Coordinate OPSEC measures with other elements of mission command warfare.

(5) Decide which OPSEC measures to implement.

Note: Action five

e. Action 5- Apply appropriate OPSEC measures.

(1) Recommend OPSEC measures to the operations cell.

(2) Verify the commander approves OPSEC measures during course of action (COA) approval.

(3) Verify the warning order (WARNO), operations plan (OPLAN), operations order (OPORD) and fragmentary order (FRAGO) address OPSEC measures and application.

(4) Monitor and evaluating the units' implementation of OPSEC.

(5) Adjust OPSEC measures, as required.

(6) Validate OPSEC as a continuous process.

(7) Assess OPSEC measures.

2. The staff led by the operations section and OPSEC officer performs OPSEC actions throughout the military decision making process (MDMP).

a. During receipt of mission, mission analysis, and COA development, the staff identifies OPSEC vulnerabilities and assess the risks they pose.

b. The staff officer tests the OPSEC measures associated with each COA by analyzing OPSEC measures from the adversary perspective.

c. The staff determines which OPSEC measures to recommend for each COA and which COA is most supportable from an OPSEC perspective.

d. The staff recommends OPSEC measures to counter the risks posed by OPSEC vulnerabilities.

e. The staff follows up on coordination done during MDMP and verifies the OPLAN and OPORD contains instructions necessary to prepare, execute, and assess the approved OPSEC measures.

3. During preparation and execution, the inform and influence activities (IIA) section and the cyber electromagnetic activities (CEMA) section, in coordination with the operations section, monitors and evaluates preparation and execution of all IIA/CEMA tasks to include the application of OPSEC measures for the approved COA by:

a. Assess execution of OPSEC measures.

b. Recommend/direct OPSEC measure changes based on assessments.

4. The IIA and CEMA sections remain alert for OPSEC indicators that may result in OPSEC vulnerabilities by using the following tools to assess OPSEC:

a. OPSEC review:

(1) Verify all staff sections review staff documents and mission command networks and systems logs to confirm protection of sensitive information.

(2) Validate standing operating procedures state which documents require OPSEC review.

(3) Validate SOP provide standards for protecting, storing, and handling sensitive information and mission command networks and systems.

(4) Verify recommendations to the appropriate staff officer, when corrective action is necessary.

b. OPSEC assessment:

(1) Determine the unit's overall OPSEC posture.

(2) Evaluate compliance of subordinate organizations with the OPSEC appendix to the IIA annex.

(3) Verify staff members conduct the OPSEC assessments and submit results and recommendations to the commander.

c. OPSEC checks:

(1) Verify the OPSEC checks are conducted.

(2) Enforce the rule of an OPSEC check to determine if the command is adequately protecting EEFI, not the effectiveness of security programs or adherence to security directives.

(3) Validate the attempt to reproduce the intelligence image that a specific operation projects to identify OPSEC vulnerabilities.

(4) Examine all of an organization's functions at all points of the operations process for the existence of OPSEC indicators.

(5) Trace the flow of information from start to finish for each of an organization's function.

(Asterisks indicates a leader performance step.)

PERFORMANCE MEASURES	GO	NO-GO	N/A
1. The staff led by the Operations Section and Operations Security (OPSEC) officer conducted the five actions of the OPSEC process.			
a. Action 1- Identified essential elements of friendly information (EEFI) from:			
(1) The commander's guidance.			
(2) The information operations (IO) estimate.			
(3) The OPSEC estimate.			
(4) The intelligence estimate.			
(5) The multi discipline counterintelligence estimate.			
(6) The higher headquarters security classification guide for the operation.			
(7) Laws and executive orders that required protection of unclassified controlled information.			
b. Action 2- Conducted analysis of adversaries.			
(1) The intent and capabilities of the adversaries to act against the planned operation.			
(2) The probable adversary objectives.			
(3) The likely adversary actions against friendly operations.			
(4) The information the adversaries already know.			
(5) The collection capabilities the adversaries possess or have access to by financial arrangement or shared ideologies, or coordinated coalitions/ alliances.			
(6) The OPSEC indicators that can be faked to deceive adversaries.			
c. Action 3- Analyzed vulnerabilities.			
(1) Identified OPSEC indicators.			
(2) Selected at least one OPSEC measure for each vulnerability (personnel, physical, cryptographic, document, special access, and automated information systems).			
(3) Identified possible OPSEC measures for each vulnerability.			
d. Action 4- Assessed risk.			
(1) Conducted a risk assessment for each OPSEC vulnerability.			
(2) Selected one or more OPSEC measure for each OPSEC vulnerability.			
(3) Determined residual risk for each OPSEC vulnerability.			
(4) Coordinated OPSEC measures with other elements of mission command warfare.			
(5) Decided which OPSEC measures to implement.			
e. Action 5- Applied appropriate OPSEC measures.			
(1) Recommended OPSEC measures to the operations cell.			
(2) Verified the commander approved OPSEC measures during course of action (COA) approval.			
(3) Verified that the warning order (WARNO), operations plan (OPLAN), operations order (OPORD) and fragmentary order (FRAGO) addressed OPSEC measures and application.			
(4) Monitored and evaluated the units' implementation of OPSEC.			
(5) Adjusted OPSEC measures, as required.			
(6) Validated OPSEC as a continuous process.			
(7) Assessed OPSEC measures.			
2. The staff led by the operations section and OPSEC officer performed OPSEC actions throughout the Military Decision Making Process (MDMP).			
a. During receipt of mission, mission analysis, and COA development, the staff identified OPSEC vulnerabilities and assessed the risks they posed.			
b. The staff officer tested the OPSEC measures associated with each COA by analyzing OPSEC measures from the adversary perspective.			
c. The staff determined which OPSEC measures to recommend for each COA and which COA is most supportable from an OPSEC perspective.			

NVG: Never

NVG Statement: None

Prerequisite Collective Task(s):

Step Number	Task Number	Title	Proponent	Status
	55-9-4805	Conduct Predeployment Activities (Battalion - Echelelons above Corps)	55 - Transportation (Collective)	Approved
	55-9-4851	Coordinate Installation/Garrison Support (Battalion - Echelons above Corps)	55 - Transportation (Collective)	Obsolete
	71-8-5113	Develop Commander's Critical Information Requirements (Battalion - Corps)	71 - Combined Arms (Collective)	Approved
	71-8-5200	Conduct Command Post Operations (Battalion - Corps)	71 - Combined Arms (Collective)	Approved

Supporting Collective Task(s):

Step Number	Task Number	Title	Proponent	Status
	71-8-2230	Provide Intelligence Support to Protection (Division - Corps)	71 - Combined Arms (Collective)	Approved
	71-8-5110	Plan Operations Using the Military Decision Making Process (Battalion - Corps)	71 - Combined Arms (Collective)	Approved
	71-8-5142	Evaluate Situation or Operation (Battalion - Corps)	71 - Combined Arms (Collective)	Approved

Supporting Individual Task(s):

Step Number	Task Number	Title	Proponent	Status
	150-718-5111	Participate in the Military Decision Making Process	150 - Combined Arms (Individual)	Approved

Supporting Drill Task(s): None

TADSS

Step ID	TADSS ID	Title	Product Type	Quantity
No TADSS specified				

Equipment (LIN)

Step ID	LIN	Nomenclature	Qty
No equipment specified			

Material Items (NSN)

Step ID	NSN	LIN	Title	Qty
No equipment specified				

Environment: Environmental protection is not just the law but the right thing to do. It is a continual process and starts with deliberate planning. Always be alert to ways to protect our environment during training and missions. In doing so, you will contribute to the sustainment of our training resources while protecting people and the environment from harmful effects. Refer to FM 3-34.5 Environmental Considerations and GTA 05-08-002 ENVIRONMENTAL-RELATED RISK ASSESSMENT

Safety: In a training environment, leaders must perform a risk assessment in accordance with FM 5-19, Composite Risk Management. Leaders will complete a DA Form 7566 COMPOSITE RISK MANAGEMENT WORKSHEET during the planning and completion of each task and sub-task by assessing mission, enemy, terrain and weather, troops and support available-time available and civil considerations, (METT-TC). Note: During MOPP training, leaders must ensure personnel are monitored for potential heat injury. Local policies and procedures must be followed during times of increased heat category in order to avoid heat related injury. Consider the MOPP work/rest cycles and water replacement guidelines IAW FM 3-11.4, NBC Protection, FM 3-11.5, CBRN Decontamination. .