

# Training and Evaluation Outline Report

**Task Number:** 71-8-6321

**Task Title:** Coordinate Defensive Information Operations (Battalion - Corps)

**Supporting Reference(s):**

Step Number	Reference ID	Reference Name	Required	Primary
	ADP 3-0	Unified Land Operations	Yes	No
	AR 380-40	POLICY FOR SAFEGUARDING AND CONTROLLING COMMUNICATIONS SECURITY	Yes	No
	FM 3-13	INFORMATION OPERATIONS: DOCTRINE, TACTICS, TECHNIQUES, AND PROCEDURES	Yes	Yes
	FM 5-0	THE OPERATIONS PROCESS	Yes	No
	FM 6-0	MISSION COMMAND	Yes	No

**Condition:** The command has received an operations plan, or warning, operations, or fragmentary order from higher headquarters and is exercising mission command. The commander has issued guidance on coordinating defensive information operations. 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 coordinates defensive information operations that ensures timely, accurate and relevant information access, establishes protection and safeguard procedures to deny adversaries the opportunity to exploit friendly information and mission command networks and systems for their own purposes.

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 task steps and performance measures that may be omitted.

**Special Equipment:** None

**Safety Level:** Low

<b>Task Statements</b>
------------------------

**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:** 09 November 2011

**Notes:** None

## TASK STEPS

1. PROTECTION: The staff, In Coordination With (ICW) the Signal Section coordinates protection of information and mission command networks and systems by implementing safeguards and planning protection of the following:
  - a. All facilities.
  - b. Intelligence collection assets and information.
  - c. Analysis and production assets.
  - d. Information dissemination and integration means.
2. The staff, ICW the Signal Section, continuously conducts risk assessment by assessing:
  - a. Information needs.
  - b. The value of information that may be compromised or lost if breached.
  - c. Information system vulnerabilities.
  - d. Threats posed by potential adversaries and natural phenomena.
  - e. Resources available for protection and defense.
3. The staff, ICW the Signal Section, plans for protection of information and mission command networks and systems across all sources of information and media. At a minimum, plans for protection of:
  - a. Hard copy (message, letter or fax).
  - b. Electronic.
  - c. Magnetic.
  - d. Video.
  - e. Imagery.
  - f. Voice.
  - g. Telegraph.
  - h. Computer.
  - i. Human.
4. The staff, ICW the Signal Section, establishes a protected information environment through development of:
  - a. Policies, which address:
    - (1) Vulnerabilities and threats.
    - (2) Friendly force capabilities.

(3) Commercial infrastructure dependencies and vulnerabilities.

b. Procedures for the implementation of policies that employ commonality.

c. Capabilities and related activities which include:

(1) Other security measures, by addressing:

(a) Personnel security.

(b) Industrial security.

(c) Physical security.

(2) Vulnerability analysis and assessment, by addressing:

(a) Internal threats.

(b) Accidental sources (magnetic emanation or electrical impulses).

(c) Natural phenomena (sunspots, hurricanes, tornadoes earthquakes, floods).

(3) Activities and technologies supporting information assurance, by addressing:

(a) Information Security (INFOSEC).

(b) Computer Security (COMPUSEC).

(c) Communications Security (COMSEC).

5. DETECTION: The staff, ICW the Signal Section and the Intelligence Section, determines means of attack detection. Elements of IO attack detection include, but are not limited to:

a. Coordinating with Service Information Warfare Centers for immediate notification of Computer Network Attacks (CNAs) and implementation of response and restoration strategies.

b. Coordinating with information system developers to ensure mission command networks and systems designed and fielded in a manner that mitigates system vulnerabilities.

c. Coordinating with information system providers and system administrators to ensure immediate reporting of system abnormalities.

d. Establishing incident reporting procedures with information and mission command networks and systems users.

e. Coordinating with law enforcement authorities (military Criminal Investigators (CI) and CI agents) regarding incident reporting procedures.

f. Coordinating with Intelligence Section to ensure effective sharing of relevant information for warning and assessment of adversary activities and timely inclusion into attack detection process. Coordination includes:

(1) Planning Indications and Warnings (I&W) to detect and report time-sensitive intelligence information.

(2) Ensuring intelligence reporting systems are streamlined to assess the IO threat in time to provide sufficient warning for action.

(3) Coordinating subordinate I&W support.

(4) Establishing reporting structure and procedures to alert managers and administrators of attack detection.

6. RESTORATION: The staff, ICW the Signal Section, establishes procedures and mechanisms for prioritized restoration of information capabilities by:

a. Coordinating for use of Computer Emergency Response Teams (CERTs).

b. Determining technical restoration capabilities.

c. Establishing automated intrusion detection systems.

d. Conducting inventory of system resources.

e. Conducting post-attack analysis.

7. RESPONSE: The Fires Section, through the Targeting planners, recommends IO attack or potential attack response by:

a. Identifying adversary actors and intent of activities.

b. Conducting analysis to determine proper response to adversary action.

c. Ensuring integration of IO attack or potential attack detection and analysis capabilities.

d. Recommending or coordinating possible national-strategic response decisions, which include:

(1) Law enforcement.

(2) Diplomatic actions.

(3) Economic sanctions.

(4) Military force (lethal and nonlethal).

(Asterisks indicates a leader performance step.)

PERFORMANCE MEASURES	GO	NO-GO	N/A
1. PROTECTION: The staff, In Coordination With (ICW) the Signal Section coordinated protection of information and Information Systems (INFOSYS), by implementing safeguards and planning protection of the following:			
a. All facilities.			
b. Intelligence collection assets and information.			
c. Analysis and production assets.			
d. Information dissemination and integration means.			
2. The staff, ICW the Signal Section, continuously conducted risk assessment by assessing:			
a. Information needs.			
b. The value of information that may be compromised or lost if breached.			
c. Information system vulnerabilities.			
d. Threats posed by potential adversaries and natural phenomena.			
e. Resources available for protection and defense.			
3. The staff, ICW the Signal Section, planned for protection of information and INFOSYS across all sources of information and media. At a minimum, planned for protection of:			
a. Hard copy (message, letter or fax).			
b. Electronic.			
c. Magnetic.			
d. Video.			
e. Imagery.			
f. Voice.			
g. Telegraph.			
h. Computer.			
i. Human.			
4. The staff, ICW the Signal Section, established a protected information environment through development of:			
a. Policies, which addressed:			
(1) Vulnerabilities and threats.			
(2) Friendly force capabilities.			
(3) Commercial infrastructure dependencies and vulnerabilities.			
b. Procedures for the implementation of policies that employ commonality.			
c. Capabilities and related activities which included:			
(1) Other security measures, by addressing:			
(a) Personnel security.			
(b) Industrial security.			
(c) Physical security.			
(2) Vulnerability analysis and assessment, which addressed:			
(a) Internal threats.			
(b) Accidental sources (magnetic emanation or electrical impulses).			
(c) Natural phenomena (sunspots, hurricanes, tornadoes earthquakes, floods).			
(3) Activities and technologies that supported information assurance, by addressing:			
(a) Information Security (INFOSEC).			
(b) Computer Security (COMPUSEC).			
(c) Communications Security (COMSEC).			
5. DETECTION: The staff, ICW the Signal Section and the Intelligence Section, determined means of attack detection. Elements of IO attack detection include, but were not limited to:			

a. Coordination with Service Information Warfare Centers for immediate notification of Computer Network Attacks (CNAs) and implementation of response and restoration strategies.			
b. Coordination with information system developers to ensure mission command networks and systems designed and fielded in a manner that mitigated system vulnerabilities.			
c. Coordination with information system providers and system administrators in order to ensure immediate reporting of system abnormalities.			
d. Established incident reporting procedures with information and mission command networks and systems users.			
e. Coordination with law enforcement authorities (military Criminal Investigators (CI) and CI agents) regarding incident reporting procedures.			
f. Coordination with Intelligence Section to ensure effective sharing of relevant information for warning and assessment of adversary activities and timely inclusion into attack detection process. Coordination included:			
(1) Planned Indications and Warnings (I&W) to detect and report time-sensitive intelligence information.			
(2) Ensuring that intelligence reporting systems were streamlined to assess the IO threat in time to provide sufficient warning for action.			
(3) Coordinated subordinate I&W support.			
(4) Established reporting structure and procedures to alert managers and administrators of attack detection.			
6. RESTORATION: The staff, ICW the Signal Section, established procedures and mechanisms for prioritized restoration of information capabilities by:			
a. Coordinated use of Computer Emergency Response Teams (CERTs).			
b. Determined technical restoration capabilities.			
c. Established automated intrusion detection systems.			
d. Conducted inventory of system resources.			
e. Conducted post-attack analysis.			
7. RESPONSE: The Fires Section, through the Targeting planners, recommended IO attack or potential attack response by:			
a. identification of adversary actors and intent of activities.			
b. Conducted analysis to determine proper response to adversary action			
c. Ensured integration of IO attack or potential attack detection and analysis capabilities.			
d. Recommended or coordinated possible national-strategic response decisions, which included:			
(1) Law enforcement.			
(2) Diplomatic actions.			
(3) Economic sanctions.			
(4) Military force (lethal and nonlethal).			

TASK PERFORMANCE / EVALUATION SUMMARY BLOCK							
ITERATION	1	2	3	4	5	M	TOTAL
TOTAL PERFORMANCE MEASURES EVALUATED							
TOTAL PERFORMANCE MEASURES GO							
TRAINING STATUS GO/NO-GO							

**ITERATION:** 1 2 3 4 5 M

**COMMANDER/LEADER ASSESSMENT:** T P U

**Mission(s) supported:** None

**MOPP:** Sometimes

**MOPP Statement:** None

**NVG:** Never

**NVG Statement:** None

**Prerequisite Collective Task(s):**

Step Number	Task Number	Title	Proponent	Status
	71-8-5110	Plan Operations Using the Military Decision Making Process (Battalion - Corps)	71 - Combined Arms (Collective)	Approved

**Supporting Collective Task(s):**

Step Number	Task Number	Title	Proponent	Status
	71-8-5111	Conduct the Military Decision Making Process (Battalion - Corps)	71 - Combined Arms (Collective)	Approved
	71-8-5130	Assess Tactical Situation and Operations (Battalion - Corps)	71 - Combined Arms (Collective)	Approved
	71-8-6700	Coordinate Protection Efforts (Brigade - Corps)	71 - Combined Arms (Collective)	Approved

**Supporting Individual Task(s):**

Step Number	Task Number	Title	Proponent	Status
	113-500-8003	Create an Information Assurance Plan	113 - Signal (Individual)	Approved
	171-170-0028	Perform Remote Access Security Procedures Using Force XXI Battle Command Brigade-and-Below / Blue Force Tracking (FBCB2 / BFT)	171 - Armor (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. .