

Training and Evaluation Outline Report

Task Number: 71-8-5010

Task Title: Conduct Information Protection (Brigade - Corps)

Distribution Restriction: Approved for public release; distribution is unlimited.

Destruction Notice: None

Foreign Disclosure: FD3 - This training product has been reviewed by the developers in coordination with the Fort Leavenworth foreign disclosure officer. This training product cannot be used to instruct international military students.

Supporting Reference(s):

Step Number	Reference ID	Reference Name	Required	Primary
	ADRP 6-0 (Change 002, March 28, 2014)	Mission Command http://armypubs.army.mil/doctrine/DR_pubs/dr_a/pdf/adrp6_0_new.pdf	Yes	No
	AR 380-5	DEPARTMENT OF THE ARMY INFORMATION SECURITY PROGRAM	Yes	No
	FM 3-38	CYBER ELECTROMAGNETIC ACTIVITIES http://armypubs.army.mil/doctrine/DR_pubs/dr_a/pdf/fm3_38.pdf	Yes	No
	FM 6-02	SIGNAL SUPPORT TO OPERATIONS	Yes	No
	FM 6-02.71	Network Operations	Yes	Yes

Condition: The command receives a mission order from higher headquarters and the commander issues guidance on conducting information protection. The command establishes communications with subordinate and adjacent units, and higher headquarters. The mission command system is operational and processing information. Some iterations of this task should be performed in MOPP 4.

Standard: The staff protects information using operations security, information assurance, computer network defense and electronic protection to safeguard and defend friendly information and information systems. The staff protects information regardless of media, telephonic, on paper, on digital devices, or traversing networks and residing on information systems. The staff protects information from time collected until utilized by the users and decision makers and in accordance with the commanders intent.

Safety Risk: Low

Task Statements

Cue: None

DANGER

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

WARNING

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: None

Notes: Note 1: Task content last updated: 22 Oct 2014

Note 2: Information Protection consists of those active or passive measures used to safeguard and defend friendly information and information systems (ADRP 6-0).

TASK STEPS

1. The staff conducts information protection as a task that resides within the mission command warfighting function.
2. The staff integrates the three parts of Information protection.
 - a. Information assurance (IA) protects and defends information systems by ensuring:
 - (1) Availability.
 - (2) Integrity.
 - (3) Authentication.
 - (4) Confidentiality.
 - (5) Nonrepudiation.
 - b. Computer network defense (CND).
 - c. Electronic protection capabilities.
3. The staff plans for information protection by:
 - a. Establishing controls during planning to reduce the risk of inadvertent disclosure of information, relying on unit standard operating procedures (SOP) and external directives, and including the following areas:
 - (1) Operations Security (OPSEC).
 - (2) Physical security.
 - (3) Risk analysis.
 - (4) Document classification marking, storage, and transporting.
 - (5) Data storage.
 - (6) Review and deliberate release of information to unified action partners or the public.
 - (7) Foreign disclosure.
 - (8) Encryption of data transmission and data at rest.
 - (9) Use of removable media.
 - (10) Protection of personally identifiable information.
 - (11) Secure architecture design.
 - b. Planning for the protection of essential elements of friendly information (EEFI) during the military decision making process (MDMP) by:
 - (1) Identifying EEFI for each course of action (COA) during COA development and analysis.

(2) Employing the OPSEC process during MDMP to establish and publish controls to protect EEFI and other information whose disclosure would provide an advantage to adversaries.

c. Defining the threat's capability to collect through validated intelligence.

4. The staff prepares for information protection by implementing controls identified during planning by:

a. Enforcing IA measures.

(1) Information systems configuration control and patching, including virus protection software.

(2) Certification of user training.

(3) Signed acceptable use policy user agreement for each user account.

(4) Password protect against unauthorized access of information systems.

b. Verifying security configurations on network information system for CND.

c. Maintaining routine SOPs, such as:

(1) Communications over unsecured means (voice and data).

(2) Use of approved shredders or complete incineration for documents and electronic media.

(3) Access control.

(4) Data backup and recovery.

(5) Alternate means of communications in case the primary plan fails.

d. Applying restricting disclosure of deception plans and measures.

e. Coordinating with intelligence, operations and public affairs staff to:

(1) Classify information.

(2) Determine sensitive information.

(3) Releasable information to the public.

f. Reviewing electronic protection (EP) controls and measures with all personnel:

(1) Electronic warfare threat.

(2) EP active and passive measures under normal conditions, conditions of threat electronic attack, or degraded networks and systems.

(3) Actions to minimize the vulnerability of friendly receivers to enemy jamming, such as:

(a) Reduced power.

(b) Brevity of transmissions.

(c) Directional antennas.

(4) Switching between redundant communications systems.

g. Coordinating electromagnetic spectrum (EMS) usage.

5. The staff protects information during operations by:

a. Reporting and investigating potential breaches or disclosures of EEFI, classified information or information whose inadvertent disclosure could otherwise create a hazard to the operation.

b. Releasing approved information through the public affairs office or to unified action partners only after formal review.

c. Coordinating with other information-related capabilities, such as:

(1) Information operations (IO)

(2) Cyber electromagnetic activities (CEMA).

(3) Military deception.

6. The signal section, network operations, and the CEMA element protect information thru CND during operations by:

a. Operating:

(1) Host-based security systems.

(2) Firewalls.

(3) Intrusion detection systems.

b. Providing IA defense in depth throughout the LandWarNet (LWN).

c. Restoring networks, systems and data to pre-event capability.

d. Conducting electronic protection tasks such as:

(1) Electromagnetic hardening.

(2) Electronic masking.

(3) Emission control.

7. The staff continually assesses protection efforts during the execution of operations by:

a. Monitoring for compromise of EEFIs.

b. Monitoring NETOPS for indications of intrusion or compromise.

Step Number	Task Number	Title	Proponent	Status
	71-8-5900	Coordinate Cyber Electromagnetic Activities (Brigade - Corps)	71 - Combined Arms (Collective)	Approved
	71-8-6300	Conduct Information Assurance (Brigade - Corps)	71 - Combined Arms (Collective)	Approved
	71-8-6320	Perform Computer Network Defense (Brigade - Corps)	71 - Combined Arms (Collective)	Approved
	71-8-6321	Coordinate Defensive Information Operations (Battalion - Corps)	71 - Combined Arms (Collective)	Approved

Supporting Individual Task(s):

Step Number	Task Number	Title	Proponent	Status
	081-68A-0475	Employ a Standard Army Management Information System	081 - Medical (Individual)	Approved
	113-367-5001	Implement Network Protection Measures	113 - Signal (Individual)	Approved
	171-630-0015	Supervise Information Management in a Battalion Command Post (CP)	171 - Armor (Individual)	Approved

Supporting Drill Task(s): None

Supported AUTL/UJTL Task(s):

Task ID	Title
ART 5.10 - INVALID	INVALID - Conduct Information Protection

TADSS

Step ID	TADSS ID	Title	Product Type	Quantity
No TADSS specified				

Equipment (LIN)

Step ID	LIN	Nomenclature	Qty
No equipment specified			

Materiel Items (NSN)

Step ID	NSN	LIN	Title	Qty
	7010-01-443-2309		Computer System, Digital: AN/TYQ-45A	1

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 ATP 5-19, Risk Management. Leaders will complete the current Deliberate Risk Assessment Worksheet in accordance with the TRADOC Safety Officer 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, Multiservice Tactics, Techniques, and Procedures for Nuclear, Biological, and Chemical (NBC) Protection, FM 3-11.5, Multiservice Tactics, Techniques, and Procedures for Chemical, Biological, Radiological, and Nuclear Decontamination. .