

Training and Evaluation Outline Report

Status: Approved

15 Nov 2011

Effective Date: 06 Oct 2016

Task Number: 71-8-6300

Task Title: Conduct Information Assurance (Brigade - Corps)

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

Destruction Notice: None

Foreign Disclosure: FD1 - This training product has been reviewed by the training developers in coordination with the Fort Leavenworth foreign disclosure officer. This training product can be used to instruct international military students from all approved countries without restrictions.

Supporting Reference(s):

Step Number	Reference ID	Reference Name	Required	Primary
	ADRP 5-0	The Operations Process	Yes	No
	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
	FM 3-13	Inform and Influence Activities	Yes	No
	FM 6-02.71	Network Operations	Yes	Yes

Conditions: 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 conducting information assurance. 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 4.

Standards: The staff, led by the Networks Operations Element, conducts information assurance through active and passive measures of information assurance, physical security, computer network defense, electronic protection, and information management to ensure the network is secure with no compromise of information. The Networks Operations Element, in conjunction with the staff, ensures timely, accurate, and relevant friendly information, denies threats the opportunity to exploit friendly information and information systems for the threat's own purposes by correctly implementing electronic protection measures prior to establishing communications, and maintaining them with 100% accuracy.

Live Fire Required: No

Objective Task Evaluation Criteria Matrix:

Plan and Prepare		Execute						Assess	
Operational Environment	Training Environment (L/V/C)	Training/Authorized	% of Leaders Present at	% of Soldiers Present at	External Eval	% Performance Measures 'GO'	% Critical Performance Measures 'GO'	% Leader Performance Measures 'GO'	Task Assessment
BDE & Above									
Dynamic and Complex (All OE Variables and Hybrid Threat)	Night	IAW unit CATS statement.	>=85%	>=80%	Yes	>=91%	All	>=90%	T
			75-84%			80-90%		80-89%	T-
Dynamic and Complex (All OE Variables and Single Threat)	Day		65-74%	75-79%	No	65-79%	<All	<=79%	P
			60-64%	60-74%		51-64%			P-
Dynamic and Complex (<All OE Variables and Single Threat)			<=59%	<=59%	<=50%	U			

Remarks: None

Notes: Task Content Last Updated 25 March 2013.

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.

Performance Steps and Measures

NOTE: Assess task proficiency using the task evaluation criteria matrix.

NOTE: Asterisks (*) indicate leader steps; plus signs (+) indicate critical steps.

STEP/MEASURE	GO	NO-GO	N/A
1. The staff, in coordination with the Network Operations (NETOPS) element, provides Information Assurance (IA) by:	N/A	N/A	N/A
Note: The capabilities for IA must be achieved at the strategic, operational, and tactical levels across all warfighting functions.			
a. Establishing functional services of IA.	N/A	N/A	N/A
(1) Access Control.	N/A	N/A	N/A
(2) Application Security.	N/A	N/A	N/A
(3) Continuity of operations.	N/A	N/A	N/A
(4) Communications Security.	N/A	N/A	N/A
(5) Risk analysis.	N/A	N/A	N/A
(6) Legal and regularity compliance.	N/A	N/A	N/A
(7) Physical security.	N/A	N/A	N/A
(8) Security in development and acquisition.	N/A	N/A	N/A
(9) Telecommunications and network security.	N/A	N/A	N/A
(10) Establishing programs and procedures.	N/A	N/A	N/A
(a) Organizational.	N/A	N/A	N/A
(b) Personnel.	N/A	N/A	N/A
(c) Hardware.	N/A	N/A	N/A
(d) Software.	N/A	N/A	N/A
(e) Media.	N/A	N/A	N/A
b. Managing the IA critical capabilities.	N/A	N/A	N/A
(1) Protection to counter vulnerabilities associated with information transport, processing, storage, and operational uses.	N/A	N/A	N/A
(2) Monitoring the network and information systems to sense and assess abnormalities and the use of anomaly and intrusion detection systems.	N/A	N/A	N/A
(3) Detection of abnormalities to include attack, damage, unauthorized access attempts and modifications to systems.	N/A	N/A	N/A
(4) Analyzing pertinent information to determine indications and warnings, providing situational awareness, evaluating system status, identifying root cause, defining courses of action, and prioritizing response and recovery actions.	N/A	N/A	N/A
(5) Responding to mitigate the operational impact of an attack, damage, or other incapacitation of a network resource or information system.	N/A	N/A	N/A
(a) Strengthening the defensive posture and operational readiness.	N/A	N/A	N/A
(b) Halting or minimizing attack and exploitation effects or damage.	N/A	N/A	N/A
(c) Defending rapid, complete attack, or exploitation characterization.	N/A	N/A	N/A
(6) Managing the technical and administrative processes in securing access to the information being transmitted over the network, or being processed/stored on information systems.	N/A	N/A	N/A
c. Implementing safeguards and controls on data networks and computer systems.	N/A	N/A	N/A
(1) Perform risk assessments of potential threats to friendly mission command systems.	N/A	N/A	N/A
(2) Correct mission command systems failures.	N/A	N/A	N/A
(3) Confirm installation of defensive software applications.	N/A	N/A	N/A
(4) Plan secondary lines of communications in case of equipment failure or enemy disruption.	N/A	N/A	N/A
d. Verifying availability, integrity, authenticity, and security of information networks, systems, use of accredited hardware, and data receipt.	N/A	N/A	N/A
e. Reacting to compromises.	N/A	N/A	N/A
f. Restoring networks, systems, and data.	N/A	N/A	N/A
2. The staff, in conjunction with the NETOPS element, denies threat access to electronic information (both communications and noncommunications):	N/A	N/A	N/A
a. Enforces operations security through:	N/A	N/A	N/A
(1) Essential elements of friendly information (EEFI) identification.	N/A	N/A	N/A
(2) Enforcement of regulations.	N/A	N/A	N/A
(3) Conduct of investigations pertaining to failures in proper handling of classified and compartment information.	N/A	N/A	N/A
(4) Analyzes friendly actions attendant to military operations and other activities to:	N/A	N/A	N/A
(a) Identify those actions that can be observed by adversary intelligence systems.	N/A	N/A	N/A
(b) Determine indicators hostile intelligence systems might obtain that could be interpreted or pieced together to derive EEFI in time to be useful to adversaries.	N/A	N/A	N/A
(c) Select and execute measures that eliminate or reduce to an acceptable level the vulnerabilities of friendly actions to adversary exploitation.	N/A	N/A	N/A

Step Number	Task Number	Title	Proponent	Status
	71-8-5310	Manage Information and Data (Battalion - Corps)	71 - Combined Arms (Collective)	Approved
	71-8-6111	Plan Operations Security (Battalion - Corps)	71 - Combined Arms (Collective)	Approved
	71-8-6320	Perform Computer Network Defense (Brigade - Corps)	71 - Combined Arms (Collective)	Approved
	71-BDE-5100	Conduct the Mission Command Operations Process for Brigades	71 - Combined Arms (Collective)	Approved
	71-CORP-5100	Conduct the Mission Command Operations Process for Corps	71 - Combined Arms (Collective)	Approved
	71-DIV-5100	Conduct the Mission Command Operations Process for Divisions	71 - Combined Arms (Collective)	Approved

OPFOR Task(s): None

Supporting Individual Task(s):

Step Number	Task Number	Title	Proponent	Status
	093-948-B138	Perform Duties as an Information Assurance Security Officer	093 - Munitions and Electronics Maintenance (Individual)	Approved
	113-367-5001	Implement Network Protection Measures	113 - Signal (Individual)	Approved
	113-394-6005	Implement Information Assurance Policy	113 - Signal (Individual)	Approved
	113-573-6001	Recognize Electronic Attack (EA) and Implement Electronic Protection (EP)	113 - Signal (Individual)	Approved
	113-616-2003	Establish ECCM Network	113 - Signal (Individual)	Approved
	113-616-2018	Conduct Electronic Counter-Countermeasures (ECCM) Network Controller (ENC) Operations within the Defense Satellite Communications System (DSCS)	113 - Signal (Individual)	Approved
	150-LDR-5100	Lead the Mission Command Operations Process	150 - Combined Arms (Individual)	Approved
	150-MC-2300	Perform Information Collection	150 - Combined Arms (Individual)	Approved
	150-MC-5124	Refine the Plan	150 - Combined Arms (Individual)	Approved
	150-MC-5125	Prepare a Fragmentary Order	150 - Combined Arms (Individual)	Approved
	150-MC-5200	Conduct Command Post Operations	150 - Combined Arms (Individual)	Approved
	805B-79R-8602	Verify Systems Compliance of Information Assurance	805B - Recruiting and Retention, Ft. Jackson (Individual)	Approved

Supporting Drill(s): None

Supported AUTL/UJTL Task(s):

Task ID	Title
ART 5.10.1 - INVALID	INVALID - Provide Information Assurance

TADSS

TADSS ID	Title	Product Type	Quantity
No TADSS specified			

Equipment (LIN)

LIN	Nomenclature	Qty
No equipment specified		

Materiel Items (NSN)

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 the current Environmental Considerations manual and the current GTA Environmental-related Risk Assessment card. 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. .