

ART 5.10.1.2 Employ Communications Security

Deny the enemy information of value that might be derived from the possession and study of telecommunications. (FM 6-02.72)
(USASC&FG)

NO.	Scale	Measure
01	Yes/No	Communications security compromises degraded, delayed, or modified unit operations.
02	Yes/No	Unit executed controlling authority functions.
03	Time	To refine and synchronize signal annex to operation order.
04	Time	To complete communications security assessment in the area of operations (AO).
05	Time	To identify improper occurrences of communications security.
06	Percent	Of increased or decreased number of security violations on combat net radios in the AO within a given time.
07	Percent	Of enemy sensor coverage in AO known to friendly force.
08	Percent	Of successful enemy attempted penetration of friendly information systems.
09	Percent	Of information system administrators and operators who have current operations security training.
10	Percent	Of identified friendly communications vulnerabilities in AO exploited by enemy actions.
11	Percent	Of electronic communications in AO encrypted or secured.
12	Percent	Of message traffic in AO exploited by enemy.
13	Percent	Of friendly information systems in AO exploited by enemy.
14	Percent	Of communications security measures previously assessed unsatisfactory that have improved based on assessment.
15	Percent	Of friendly operations conducted in a restrictive emission control environment.
16	Percent	Of units, installations, and agencies in AO operating from a common signal operation instructions.
17	Percent	Of unit communications systems requiring more than

		one encryption system.
18	Percent	Of communications systems using encryption.
19	Percent	Of systems that include communications security in communications network planning.
20	Number	Of communications security incidents reported.
21	Number	Of security violations on combat net radios in the AO.
22	Number	Of teams fielded to monitor friendly communications systems.
23	Number	Of interceptions of friendly communications during planning and execution.
24	Number	Of redundant communications paths available to connect operational information systems.

Supporting Collective Tasks:

Task No.	Title	Proponent	Echelon
06-6-4008	Develop the Physical Security Plan	06 - Field Artillery (Collective)	Brigade
07-5-1005	Conduct Scheduled Communications	07 - Infantry (Collective)	Team (TOE)
34-2-0011	Maintain Operations Security	34 - Combat Electronic Warfare and Intelligence (Collective)	Company
34-4-1720	Establish the Tactical Exploitation System (TES) Communications and Reporting Architecture	34 - Combat Electronic Warfare and Intelligence (Collective)	Section
34-5-3062	Disengage Common Ground Station (CGS) Communications	34 - Combat Electronic Warfare and Intelligence (Collective)	Team (TOE)
63-9-1100	Maintain Tactical Communications (Battalion-Echelons Above Corps)	63 - Multifunctional	Echelons Above

		Logistics (Collective)	Corps
--	--	---------------------------	-------