

## ART 5.10.1.1 Ensure Information Security

Deny the enemy access to electronic information (both communications and noncommunications) that could be used to identify friendly capabilities and intentions. (FM 3-13) (USACAC)

<b>NO.</b>	<b>Scale</b>	<b>Measure</b>
01	Yes/No	Signal security compromises degraded, delayed, or modified unit operations.
02	Yes/No	Firewalls, virus protection software, or other information protection measures protected unit information systems.
03	Time	To refine and synchronize signal and information operations (IO) annexes to operation order.
04	Time	To complete operations security (OPSEC) assessment in the area of operations (AO).
05	Time	To identify improper occurrence of signal security.
06	Time	For appropriate information response teams to respond, identify, and correct information system failures attributed to enemy offensive IO or criminal activity.
07	Percent	Of increased or decreased number of security violations on combat net radios in the AO within a given time.
08	Percent	Of successful enemy attempted penetration of friendly information systems.
09	Percent	Of emitter system administrators and operators who have current OPSEC training.
10	Percent	Of enemy sensor coverage in AO known to friendly force.
11	Percent	Of identified friendly vulnerabilities in AO exploited by enemy actions.
12	Percent	Of electronic communications in AO encrypted or secured.
13	Percent	Of message traffic in AO exploited by enemy.
14	Percent	Of friendly emitters in AO exploited by enemy.
15	Percent	Of signal security measures previously assessed unsatisfactory that have improved based on assessment.
16	Percent	Of friendly operations conducted in a restrictive emission control environment.

17	Percent	Of units, installations, and agencies in AO operating from a common signal operation instruction.
18	Percent	Of unit communications systems required to maintain more than one encryption system.
19	Number	Of security violations on combat net radios in the AO.
20	Number	Of teams fielded to monitor friendly emitters.
21	Number	Of interceptions of friendly communications during planning and execution.
22	Number	Of instances when frequency allocation or frequency management fails to prevent signal fratricide.

### Supporting Collective Tasks:

Task No.	Title	Proponent	Echelon
06-6-4008	Develop the Physical Security Plan	06 - Field Artillery (Collective)	Brigade
34-4-1720	Establish the Tactical Exploitation System (TES) Communications and Reporting Architecture	34 - Combat Electronic Warfare and Intelligence (Collective)	Section
34-6-0501	Implement Information Security Procedures	34 - Combat Electronic Warfare and Intelligence (Collective)	Brigade
34-6-0502	Implement a Personnel Security Program	34 - Combat Electronic Warfare and Intelligence (Collective)	Brigade
71-8-6321	Coordinate Defensive Information Operations (Battalion - Corps)	71 - Combined Arms (Collective)	Corps