

**Report Date:** 29 Apr 2012

**Summary Report for Individual Task  
091-94E-1034  
Determine COMSEC Insecurities  
Status: Approved**

---

DISTRIBUTION RESTRICTION: Approved for public release; distribution is unlimited.

DESTRUCTION NOTICE: None

**Condition:** In an operational environment, your supervisor tasks you to identify potential COMSEC incidents in a communications security (COMSEC) equipment repair facility. At your disposal you have the following reference material: AR 380-40, TB 380-41, DA Pam 25-380-2 and Local Standard Operation Procedure (SOP).

**Standard:** 1. Identified with 100% accuracy all potential COMSEC incidents within the repair facility. 2. Immediately alerted supervisor of all potential incidents for reporting.

**Special Condition:** None

**Special Standards:** None

**Special Equipment:**

**Safety Level:** Low

**MOPP:**

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

**Cue:** Your supervisor tasks you to identify potential COMSEC incidents in a communications security (COMSEC) repair facility.

<b>DANGER</b>
None

<b>WARNING</b>
None

<b>CAUTION</b>
None

**Remarks:** None

**Notes:** None

## Performance Steps

1. Identify potential Physical incidents.

a. Potential incidents include but are not limited to: loss, theft, loss of control, capture, recovery by salvage, tampering, or unauthorized viewing, access or photography.

b. Cryptographic Items (CCI), keyed or unkeyed, are included and will be reported accordingly.

2. Identify potential Cryptographic incidents.

a. Any equipment or software malfunction, human error by an operator or COMSEC Custodian that adversely affects the cryptosecurity of a machine, auto-manual, or manual cryptosystem.

b. Use of COMSEC keying material that is compromised, superseded, defective, or previously used (and not authorized for reuse) or incorrect application of keying material.

3. Identify potential Personnel incidents.

a. Known or suspected absence without leave, defection, espionage, treason, or sabotage by a person having access to or a detailed knowledge of COMSEC information.

b. Any occurrence that may jeopardize the security of COMSEC material or the information it protects.

4. Report potential incidents to supervisor.

(Asterisks indicates a leader performance step.)

**Evaluation Preparation:** Ensure all items required in the condition statement (or appropriate substitutions) are on hand and all safety requirements are met.

PERFORMANCE MEASURES	GO	NO-GO	N/A
1. Identified potential Physical incidents.			
2. Identified potential Cryptographic incidents.			
3. Identified potential Personnel incidents.			
4. Reported potential incidents to supervisor.			

### Supporting Reference(s):

Step Number	Reference ID	Reference Name	Required	Primary
	AR 380-40	POLICY FOR SAFEGUARDING AND CONTROLLING COMMUNICATIONS SECURITY	Yes	No
	AR 380-5	DEPARTMENT OF THE ARMY INFORMATION SECURITY PROGRAM	No	No
	AR 380-53	Communications Security Monitoring	No	No
	AR 380-67	The Department of the Army Personnel Security Program (*RAR 001, 08/04/2011)	No	No
	PAM 25-380-2	(O) SECURITY PROCEDURES FOR CONTROLLED CRYPTOGRAPHIC ITEMS	No	No
	TB 380-41	Security: Procedures for Safeguarding, Accounting and Supply Control of COMSEC Material.	Yes	No

**Environment:** All operations must conform to the Army Environmental Program, TC 3-34.489 (The Soldier and the Environment), 3-34.5 (ENVIRONMENTAL CONSIDERATIONS {MCRP 4-11B}), AR 200-1 Environmental Protection and Enhancement), local, state, and federal environmental policies, The Clean Air Act (CAA), CAA amendments, National Ambient Air-Quality Standards (NAAQS), as well as OSHA Hazard Communication Standard for Industry, 29 CFR, part 1910.

**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. Incidental to Army operations and activities, all operations must provide for public safety, safe and healthful workplaces, procedures and equipment. Observe all safety precautions when using lifting devices and handling heavy parts. Observe all safety and/or environmental precautions regarding electricity, radiation, radio frequency (RF), fuel, lubricants, high pressures, and refrigerants. Provide ventilation for exhaust fumes during equipment operation and use hearing protection when required in accordance with AR 385-10 (The Army Safety Program), The Clear Air Act (CAA), CAA amendments, National Ambient Air Quality Standards (NAAQS), and the OSHA Communication Standard.

**Prerequisite Individual Tasks :** None

**Supporting Individual Tasks :** None

**Supported Individual Tasks :** None

**Supported Collective Tasks :**

Task Number	Title	Proponent	Status
43-2-4552	Perform Field Maintenance	09 - Ordnance (missiles and munitions) (Collective)	Approved
09-2-4000	Perform Direct Support Maintenance Operations (EAD)	09 - Ordnance (missiles and munitions) (Collective)	Approved

**ICTL Data :**

ICTL Title	Personnel Type	MOS Data
94E Radio Communications Security Repairer Skill Level 1	Enlisted	MOS: 94E, Skill Level: SL1