

27 MARCH 1998



Communications and Information

***DEPLOYABLE COMMUNICATIONS
STANDARDS-DEPLOYED
COMMUNICATIONS SECURITY (COMSEC)
MANAGEMENT STANDARD***

COMPLIANCE WITH THIS PUBLICATION IS MANDATORY

NOTICE: This publication is available digitally on the PACAF WWW site at: <http://www.hqpacaf.af.mil/publications>. If you lack access, contact your Publishing Distribution Office (PDO).

OPR: HQ PACAF/SCMC
(SMSgt Brian W. Snyder)

Certified by: HQ PACAF/SCM
(Col Thomas J. Latino)

Pages: 5
Distribution: F

This instruction implements policy found in Air Force Policy Directive 33-1, *Command, Control, Communications, and Computer (C4) Systems*. This volume standardizes procurement and management of COMSEC material during deployable operations. It provides general guidance for deployable communications unit engineering and deployment planning branches, base-level COMSEC managers, and deployed COMSEC responsible officers (CROs). It also provides essential information on the overall management of COMSEC material in the deployable environment. This publication applies to PACAF active PACAF-gained active deployable communications units. This publication does not apply to ANG and USAFR units and members.

1. General. Deployment planners/engineers must be aware of the COMSEC requirements needed to support the communications requested by the subscriber. These COMSEC requirements will be dependent on the mission, with whom the subscriber needs to communicate, and the classification of the traffic being handled.

2. Predeployment. The following steps should be accomplished, as necessary, during predeployment activities:

2.1. Engineering and Deployment Planning Branches:

- 2.1.1. Coordinate with appropriate tasking agency on all COMSEC keying material/documents required to support the tasking.
- 2.1.2. Coordinate point-to-point encrypted links with the appropriate authorities and distant ends.
- 2.1.3. Coordinate with DCS entry station/nodes on type(s) of required COMSEC material.

2.1.4. Send the planned COMSEC keying material requirements to the communications operations officer at each end of the encrypted intertheater link no later than (NLT) 60 days prior to the start date of the deployment.

2.1.5. Provide equipment requirements to CRO/Unit COMSEC manager NLT 15 days prior to deployment.

NOTE:

If the required COMSEC material is held at the base COMSEC account, notifying the manager 10 days prior to the start date of a deployment is sufficient. However, if the COMSEC material is not held at the account, or other link's accounts, or additional copies must be obtained, sufficient lead time must be given to obtain the material from another account or to order the material from DIR CRYPTO MGT SA-ALC/LTMKK. When ordering COMSEC material from DIR CRYPTO MGT SA-ALC/LTMKK, extra delivery time (sometimes up to 45 days for the courier time alone) is required for COMSEC accounts located in areas where irregular courier schedules exist.

2.2. Base COMSEC Manager:

2.2.1. Coordinate with the COMSEC planner to ensure all required material is available.

2.2.2. Identify shortfalls/limitations.

2.2.3. Coordinate with the deployed site CROs regarding their requirements.

2.2.4. Send an intent-to-use message to the Joint Staff ICP manager at least 10 days prior to start date of deployment if the tasking requires ICP keying material.

2.3. Unit Commander:

2.3.1. Assign a primary and alternate deployed CRO for each site requiring COMSEC.

2.3.2. Review planned COMSEC requirements to ensure they can be met with the tasked equipment.

NOTE:

Ensure COMSEC requirements are passed from the COMSEC planners to the base COMSEC manager, deploying CROs, and affected facility chiefs.

2.4. COMSEC Responsible Officer:

2.4.1. Coordinate with base COMSEC manager on all actions required to receipt for deployed COMSEC material.

2.4.2. Coordinate with deploying squadron operations officer, alternate CRO, and facility chiefs on requirements.

2.4.3. Ensure deployed operating instructions include procedures for the control, protection, and accounting of COMSEC, equipment and keying material.

2.4.4. Brief COMSEC user on procedures and requirements.

2.4.5. Ensure all required COMSEC material is picked up.

2.4.6. Ensure at least one primary and one alternate COMSEC user is appointed for each facility.

2.4.7. Ensure all documentation and forms, e.g., AFCOMSEC Form 16, **Daily Shift Inventory**; SF 153, **COMSEC Material Reports**, access and requirements letters, etc., are accurate and current.

2.4.8. Review users six-part folders for accuracy during material pick-up.

2.4.9. Ensure facility operating instructions include end-of-day/shift security checks.

2.5. Facility Chief (Optional):

2.5.1. Appoint deployed COMSEC user for each facility.

2.5.2. Ensure COMSEC user coordinates with the deploying CRO to determine facility requirements.

2.5.3. The facility COMSEC user will ensure the pick-up, transportation, accountability, use, and destruction of their respective COMSEC materials.

3. Deployment. The deploying CRO is the focal point for all COMSEC matters during the deployment and should be solely dedicated to that task. The CRO:

3.1. Advises the site commander on all COMSEC matters.

3.2. Ensures an adequate supply of COMSEC material is transported to the deployed location. (Current supply plus 90 days is necessary for extended deployments.)

3.3. Ensures COMSEC users handle COMSEC according to applicable directives.

3.4. Performs COMSEC inspections using AFCOMSEC Form 19 within 72 hours of facility activation. COMSEC inspections must also be conducted every 90 days and prior to departure of current CRO. This policy must be in effect until the operation is terminated.

3.5. Ensures all superseded keying material is properly destroyed during the deployment.

3.6. Ensures all destruction documentation is completed after destruction. Returns the destruction report(s) to the appropriate COMSEC account.

3.7. Coordinates Emergency Action Plans (EAPs) with deployed COMSEC manager and ensures dry runs are performed within 24 hours upon arrival on site for operational "real world" deployments or from the start of S-hour for exercises.

3.8. Is prepared to request additional required COMSEC materials beyond the normal supply, as needed.

3.9. Ensure COMSEC insecurities are immediately reported to the controlling authority and, if applicable, to the home station COMSEC manager.

4. Redeployment. At termination of operations, the CRO will perform the following:

4.1. Ensure superseded materials are destroyed and obtain a copy of destruction report.

4.2. Ensure inventories are filled out properly before shipment.

4.3. Make sure materials are properly prepared for shipment.

4.4. The base COMSEC manager debriefs, as needed, the deployed CRO/user on all COMSEC matters.

5. Post Deployment:

- 5.1. Upon arrival at home station, users turn in their COMSEC documents, future materials (when applicable), etc., to the unit's CRO or COMSEC manager.
- 5.2. CROs will return destruction reports to the COMSEC account.

NOTE:

CROs will ensure deployed six-part folders are purged of outdated materials and all hand receipts are cleared.

BERNARD K. SKOCH, Colonel, USAF
Director, Communications and Information

Attachment 1**GLOSSARY OF REFERENCES*****References***

A1.1. Combat communications planners, COMSEC managers, and COMSEC responsible officers should be familiar with the following:

Table of Allowance 420, Wartime Tasked Communications Organizations (AFIND 10)

AFKAG-1, Air Force COMSEC Communications Security Policy and Procedures (available through COMSEC channels)

AFKAG-14, Index and Status of COMSEC Operations, Exercise, and Training Material (available through COMSEC channels)

AFKAG-11, Index and Status of KG-84 Operational, On-the-Air Test and Maintenance Test Keying Systems (available through COMSEC channels)

AFKAG-13, Index and Status of COMSEC General, Operating, and Maintenance Manuals (available through COMSEC channels)

Intertheater COMSEC Package (ICP) Distribution Scheme (available through COMSEC channels)

Defense Information Systems Agency Contingency/Exercise Plan 10-93 (available through plans channels)

AFI 33-211, User Requirements (Indexed in AFIND 2)

A1.2. In addition to the above listed documents, COMSEC custodians and managers must be familiar with the following:

AFI 33-210, Cryptographic Access Program (AFIND 2)

AFSSI 4001, (FOUO) Control of Top Secret Keying Material (AFIND 5)

AFI 33-212, Reporting COMSEC Incidents (AFIND 2)

AFI 33-213, COMSEC Functional Review Program (COMSEC Inspections) (AFIND 2)