

20 May 1998



Communications and Information

COMMUNICATION SECURITY

COMPLIANCE WITH THIS PUBLICATION IS MANDATORY

NOTICE: This publication is available digitally on the HQ AFRC WWW site at: <http://www.afrc.af.mil> and the AFRCEPL (CD-ROM) published monthly.

OPR: 931 OSF/IN (Maj Steven L. Kett)

Certified by: 931 OSF/CC
(Maj Raymond A. Kozak)

Pages: 3

Distribution: F

This instruction details specific procedures for the handling, controlling, protection, inventorying, incident reporting, and the destruction of Communications Security (COMSEC) assets and to ensure the maximum protection of these materials. This instruction implements AFRPD 33-2, *Information Protection*.

1. General. Accountability of all COMSEC material is the responsibility of the COMSEC Responsible Officer (CRO), Alternate COMSEC Responsible Officer (ACRO), or personnel authorized access to COMSEC material. During fires, natural disasters, or covert threats, all COMSEC material will be handled in accordance with the appropriate COMSEC Emergency Action Plan (EAP).

2. Training. Upon initial appointment, and annually thereafter, the CRO and ACRO will be trained by the personnel assigned to the COMSEC main account. It is then the responsibility of the CRO and ACRO to train their users and document this training on an Air Force Communications Security Form 30, CRO and User Training Checklist. A semiannual review and dry run of this instruction and EAPs are required. This review must be documented for review by inspection personnel assigned to the Major Command (MAJCOM).

3. COMSEC Pickup and Handling:

3.1. Pickup of COMSEC material will be scheduled for the last Wednesday of every month.

3.2. To receipt for or delivery of COMSEC material to and from the Base COMSEC Main Account is the responsibility of the CRO or the ACRO. It is also their responsibility to perform "A" page checks, post amendments to the COMSEC documents, and destroy/witness destruction of COMSEC material. The CRO and ACRO(s) will be identified by letter to the Base COMSEC Account Custodian and these letters will be posted in the COMSEC letter file that is kept in the safe. No other personnel will perform these actions.

3.3. A SF 153, **COMSEC Material Report**, will be utilized when receiving COMSEC material. This document will be prepared by the COMSEC Main Account and ready upon arrival to the COMSEC vault. Match each document against the SF 153. Ensure the "Short Title", "Edition", "Quantity", and "Register Number(s)" match. Never sign a SF 153 that has material incorrectly listed.

3.4. Issue COMSEC material only to authorized personnel. A list of personnel authorized to receive COMSEC material will be maintained in the COMSEC folder.

3.5. All COMSEC material will be stored in the safe unless under constant surveillance of persons authorized access to the material.

3.6. All COMSEC material removed from the safe will be annotated on a SF 153.

3.7. When COMSEC material is received, it will be immediately placed in the safe and added to the inventory on AFCOMSEC Form 16 by entering the "Short Title", "Edition", "Quantity", and "Register Number(s)" of each item.

3.8. COMSEC materials will be transported within a locked or sealed briefcase, closed bag, or suitable container while on or off base.

4. Safe and Inventory Procedures:

4.1. The classification of the safe combination will be equal to the highest classification of material in the safe.

4.2. The safe combination will be changed at least every 12 months and as required by AFI 33-211.

4.3. Maintain SF 700, **Security Container Information**. Record date of last combination change on form and store in locking drawer of safe.

4.4. Maintain SF 701, **Activity Security Checklist**.

4.5. Maintain SF 702, **Security Container Check Sheet**, to show who unlocked, locked, and checked the safe. Different individuals should lock and check the safe, unless another person is not reasonably available. Destroy the old form once the new one has been initiated.

4.6. The safe will be inventoried on the shift it was opened. The inventory will be taken just prior to closing the safe.

5. COMSEC Destruction Procedures:

5.1. Ensure identity and completeness of all material to be destroyed. Maintain a record on SF 153, in duplicate, and file duplicate copy in the COMSEC folder. The original copy will be hand carried to the COMSEC custodian.

5.2. Destroy each code as soon as possible after supersession or keying as applicable, not to exceed 12 hours after supersession unless workcenter is closed, i.e., weekend, holiday, in which case destroy on next duty day. Two authorized individuals must be present during the destruction.

5.3. Compare the COMSEC material to be destroyed with the destruction report and have the witness verify that the correct material is being destroyed.

5.4. Destroy codes/material by burning IAW AFI 33-211 or return it to the COMSEC Center for shredding. When destroying code pages, annotate the code(s) destroyed on the segments/issue record.

6. Incident Reporting Procedures:

6.1. The importance of reporting all known or suspected COMSEC incidents immediately cannot be overemphasized. Each user/agency must immediately report any occurrence that may jeopardize the security of COMSEC material to the CRO or ACRO. If transient personnel are involved in a possible incident, provide their names, ranks, organization, and all known pertinent information about the individual(s) to the CRO, ACRO, or COMSEC Manager.

6.2. Report all of the following:

6.2.1. Physical incidents: Loss of control, theft, recovery by salvage, improper destruction, tampering, unauthorized viewing, access, or copying.

6.2.2. Personnel incident: Any capture, attempted recruitment, known or suspected control by a hostile intelligence entity, or defection of an individual who has access to COMSEC information.

6.2.3. Cryptographic incident: Any equipment malfunction or operator error that threatens the security of a system or equipment, including the unauthorized use of COMSEC keying material or equipment.

7. Classified Waste. To ensure that classified material does not leave the area, wastebaskets will be inspected prior to disposing of trash.

8. Personnel. Personnel who are due to permanently depart McConnell AFB will be removed from the COMSEC access list no later than 30 days prior to their departure date. All personnel who have signed for classified COMSEC material must ensure that the responsibility is transferred to another COMSEC User or Alternate at least 30 days prior to their departure date. This will be coordinated through the Base COMSEC Custodian.

DEAN J. DESPINOY, Colonel, USAFR
Commander