

15 May 1997



Security

INFORMATION SECURITY PROGRAM

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: 73 AS/DOTF (SMSgt Kevin Pomeroy)

Certified by: 932 OG/CC (Col Rudolph C. Schwartz)

Supersedes 932 AWI 31-1, 1 October 1995

Pages: 4
Distribution: F

This instruction establishes the Information Security Program for the 932d Airlift Wing (AW). It provides information on the control of classified material and information security to all 932 AW members. It assigns responsibilities to the wing security manager, squadron commanders, and squadron security managers for the Information Security Program. It implements Air Force Policy Directive (AFPD) 31-4, AFPD 31-5, Air Force Instruction (AFI) 31-401, DOD 5200.1-R, and AFI 31-501.

SUMMARY OF REVISIONS

This revision changes the TEMPEST acronym to EMSEC (para 3.12), 375 CG/SCPT to 375 CPSS/SCO (para 4.1) and identifies the classified copier in the 932 AW. A (I) indicates revisions from the previous edition.

1. General. Only personnel with access, appropriate clearance levels, signed Standard Form (SF) 312, **Classified Information Nondisclosure Agreement**, and the need-to-know are granted access to classified material; however, all assigned personnel are responsible for protecting both classified and unclassified information in their possession. The 932 AW Commander appoints in writing a wing security manager and an alternate security manager. Squadron commanders shall appoint squadron security managers and alternates.

1.1. The wing security manager is the focal point with the host security agency for the overall program. The wing security manager is responsible for security clearances, tracer actions, briefings and briefing actions, disseminating security information, providing general expertise, and monitoring host-base requirements. The squadron security managers are responsible for quarterly and annual briefings, and disseminating security information to personnel in their respective squadron.

1.2. In the event access to TOP SECRET (TS) information is needed, squadron commanders are responsible for actions and control of all TOP SECRET materials.

1.3. A SECRET (S) clearance is required for the wing security manager and all appointed squadron security managers. Squadron security managers are focal points for the security program within their respective squadrons; they submit security clearance actions to the wing security manager. Actions include correcting and updating erroneous data.

1.4. All squadron security managers shall produce quarterly training plans and use them to conduct security training.

2. Clearance Requirements:

2.1. Normally Reserve personnel are cleared for access on a need-to-know basis to the level of SECRET.

2.2. The squadron security manager will maintain, update, and review the squadron Automated Security Clearance Access roster (ASCAS).

2.3. Civilian personnel are cleared for the level of security required by the sensitivity of their respective civilian position. An Air Reserve Technician (ART) in a non-sensitive position may hold a SECRET clearance as a reservist and only a favorable investigation as a civilian employee.

2.4. All information impacting an individual's suitability to maintain a security clearance, such as substance abuse, UCMJ action, and civil action, must be reported to the security manager for required review.

3. Procedures Within the 932 AW for Storage of Classified Material:

3.1. The 932 MSS/SCB (Communications and Information) and 932 MSS/DPMD (Personnel Systems/Readiness) may store clearly marked CONFIDENTIAL and SECRET material in safes SCB-2, SCB-2a, and DP-4, when addressees are unavailable.

3.2. The 932 CES (Civil Engineer Squadron) may store information in safe CES-3, with the exception of paragraph 3.4.

3.3. The 932 AW/XP (Plans) may store information in safe XP-5, with the exception of paragraph 3.4.

3.4. The 932 OG/CC (Operations Group Commander) may store CONFIDENTIAL and SECRET information in safe DOTF-1, including SORTS material. SORTS material may also be stored in safes SCB-2, or DP-4, when access to safe DOTF-1 is not available.

3.5. All approved safes in the 932 AW (DOTF-1, SCB-2, SCB-2a, CES-3, DP-4, XP-5) are authorized storage containers for CONFIDENTIAL and SECRET materials.

3.6. Storage and maintenance of all classified records are accomplished IAW AFMAN 37-193, *Records Disposition Schedule*, and must be approved by the 932 AW records manager.

3.7. The combination of safes DOTF-1, SCB-2, SCB-2a, CES-3, DP-4, and XP-5 will be logged on SF Forms 700, **Security Container Information**, and the combination locations will be known by the wing security manager and appropriate safe custodians.

3.8. Procedures for receipt of classified materials:

3.8.1. Except for high-precedence messages, generally picked up at the base communications center, most classified material is delivered through the Base Information Transfer Center (BITC). Incoming classified material is signed for by the appropriately cleared wing mailroom personnel, when required. When they are absent, names of other designated personnel are clearly posted in the mailroom.

3.8.2. Classified material received in the wing mailroom will remain unopened, if adequately addressed, until the appropriate addressee receives the material.

3.8.3. Upon receipt of CONFIDENTIAL, SECRET, or otherwise accountable material, wing mailroom personnel will notify the appropriate addressee. If the addressee is unavailable, material is placed in safe SCB-2, or SCB-2a until it is picked up. Accountable mail will be distributed only to personnel who have been authorized in writing to receive such material.

3.8.4. While classified material is in the possession of the addressee, it shall be properly protected.

3.9. Classified information may be reproduced only on a copier approved for classified reproduction. The classified copier for the 932 AW is located in Bldg 3650, room 229.

3.10. Classified material can be transmitted using a formatted message sent through the base communication center or by using the BITC.

3.11. Do not remove classified material from Building 3650 without prior approval. When it is removed, it shall be transported only on base, covered and enclosed in an envelope or briefcase, and hand carried to the point of delivery. Off-base transport shall be authorized only by the base commander when an emergency exists (AFI 31-401).

3.12. Prepare typewriter-generated SECRET and CONFIDENTIAL material as prescribed. The preparation of classified material (including SORTS) on EMSEC-approved computers is the responsibility of the appropriate 932 AW office or subordinate squadron.

3.13. Custodians review their files at least semiannually to ensure any classified material eligible for destruction is destroyed as soon as possible (IAW AFMAN 37-139).

3.14. Personnel having been granted access to classified material who question the classification of particular information should contact the unit security manager or wing security manager. If justified, the classification may be (anonymously) challenged to the originator.

3.15. The squadron security manager will evaluate and determine all essential element friendly identifiers (EEFIs).

4. Procedures for Handling Improperly Classified Electronic Mail (E-MAIL). Once you suspect the e-mail is possibly classified, take the following actions:

4.1. Contact the network system administrator, the wing security manager, and the local communications system security office (375 CPSS/SCO, 6-5075) and inform them of your discovery of potentially classified information being improperly transmitted over unsecured means. Do not delete the message from your mailbox until instructed to do so by either your local computer systems security office or the local network system administrator. The local network system administrator and the local communications systems security office will need an electronic copy of the message to track it down within the network.

- 4.2. Refer to the “To”, “From”, and “Cc” lists on the e-mail to determine who else has encountered the message (the “addressees”).
- 4.3. As soon as possible, inform all addressees that the message may be classified, but that they should not delete it.
- 4.4. Instruct all addressees to retrieve, mark, and protect any printouts of the message IAW DOD 5200.1-R, Chapters IV and V.
- 4.5. Make a list of the addressees, and indicate what each person did with the message.
- 4.6. If the message was saved to a floppy disk, instruct the person to mark and protect the floppy disk at the proper level of classification IAW DOD 5200.1-R, Chapter VI.
 - 4.6.1. The network systems administrator or the local communications system security office will send someone to your office to resolve the situation. Have the list(s) you created above ready when the representative arrives. A preliminary inquiry shall be initiated to determine the circumstances surrounding the security incident IAW DOD 5200.1-R, Chapter VI.
 - 4.6.2. The representative will track down and remove all copies of the message from the network. They will also collect all floppy disks on which the message resides and remove the message. If the message was saved to a person’s hard drive, SC representatives will remove it using special software approved for this purpose. All affected personnel will be instructed to completely power-down their computers to purge the message from their system’s memory.
 - 4.6.3. The representative and/or appointed preliminary inquiry official will interview you to determine:
 - 4.6.3.1. What exactly happened.
 - 4.6.3.2. Whether the incident damaged national security.
 - 4.6.3.3. What can be done to minimize or negate any damage.
 - 4.6.3.4. Suitable corrective action to prevent future incidents.
 - 4.6.3.5. The preliminary inquiry official will prepare a report to the appointing official. If a formal investigation is not warranted, the appointing official closes the inquiry.

ALAN M. MITCHELL, Col, USAFR
Commander