

21 December 1998

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: 305 RQS/SCB
(MSgt Terrilyn Wailani-Mulloy)
Supersedes 305 RQS 31-401, 31 October 1997

Certified by: 305 RQS/CC (Col Kent D. Clark)

Pages: 10
Distribution: F

This instruction implements AFPD 31-4. It is to be used in conjunction with AFI 31-401, AFJI 31-404, AFI 31-501, ACCPAM 31-101, as supplemented 305 RQSI 31-501, and 305 RQSI 33-301. It establishes policy for security education, physical security, and handling classified information in the 305th Rescue Squadron (RQS). All personnel assigned to the 305 RQS are responsible for complying with this instruction.

SUMMARY OF REVISIONS

This revision updated references and titles. Added the requirement for NATO briefings. Added expiration for DD Forms 2501. Updated safe locations. Added procedures for removal of information from IN vault. Updated copier information. A (I) indicates revision from previous edition.

1. Security Education. The unit security manager will ensure all information security training is accomplished as required. Once training is conducted, the Unit Training Manager (LGLT) will be notified to update Core Automated Maintenance System (CAMS). Newly-assigned civilian and military personnel will process in through the security manager or alternate. The individual's security clearance will be validated or a clearance request will be initiated.

1.1. Phase I Training. This training is required for all newly-assigned personnel. ACCPAM 31-101, *Physical Security Awareness Training*, will be used as the guide for this training. Training may be supplemented by local training aids. Phase I Training will be accomplished prior to issuance of an AF Form 1199, **Restricted Area Badge**. All newly-assigned personnel will be provided initial Phase I training.

1.2. Phase II Training. This training is required for personnel identified on the Automated Security Clearance Access System (ASCAS) as having access to classified. The following will be included in Phase II Training:

- 1.2.1. Adverse affects of unauthorized disclosure.
- 1.2.2. Marking, storage, destruction, dissemination, and transmission of classified information.
- 1.2.3. Challenging classification decisions.
- 1.2.4. Foreign intelligence techniques and reporting criteria.
- 1.2.5. Penalties for engaging in espionage activities.
- 1.2.6. Prohibition of discussing classified information on unsecured telephones, radios, and facsimiles.
- 1.2.7. Penalties for gross negligence or willful disregard of the Information Security Program.
- 1.2.8. Continuous Evaluation Program.

1.3. Recurring Training. The security manager with LGLT collaboration will schedule this training according to AFCAT 36-2223, *USAF Formal Schools*.

1.4. Employment Termination Briefing. The security manager will be notified as far in advance as possible of impending separations, discharges, or resignations. AF Form 2587, **Security Termination Statement**, will then be initiated by the security manager to debrief both civilian and military personnel of their responsibilities on previously gained classified information. Completed AF Forms 2587 will be maintained by the security manager for a period of 2 years.

2. Unauthorized Absences. The immediate supervisor will determine if an individual who has access to classified material meets the criteria for unauthorized absence. When this determination is made, the supervisor will notify the commander or security manager. The security manager will be notified immediately of any derogatory information that may impact the security clearances (continued access to classified information) of unit personnel.

2.1. When it is discovered that an individual assigned to the 305 RQS who has access to classified information is on unauthorized absence, the individual's supervisor will make every reasonable effort to locate the individual. If after 24 hours and the individual is not located, the individual's supervisor must notify the security manager.

2.2. The security manager will ensure the classified information to which the individual had access is inventoried. This will be conducted by the safe custodian or any person who has access to the same material and is knowledgeable of the material.

2.3. After the inventory, an inquiry will be initiated and a report made to the DOD component counterintelligence organization and servicing AF Office of Special Investigation, if appropriate.

3. Briefings:

3.1. Foreign Travel Briefing. The commander or designated representative will brief unit members possessing TOP SECRET clearances deploying outside of the continental United States for government or personal travel. The briefing will be conducted from the outline in AFI 31-401, *Managing the Information Security Program*.

3.2. Classified Briefings. Procedures for conducting classified briefings will be accomplished following guidance in AFI 31-401 and the 305 RQS Secure Briefing Checklist (Attachment 1).

3.3. NATO Briefings. The commander appoints the security manager to conduct NATO briefings in accordance with AFI 31-401 and uses AF Form 2583, **Request for Personnel Security Action**, to document briefing.

4. Physical Security:

4.1. Storage:

4.1.1. Classified material will be locked in an approved security container when not under positive control of authorized individuals. Cover sheets for classified material will be removed prior to returning the material to secure storage. Security containers will NEVER be left open or unlocked when unattended.

4.1.2. Container custodians will verify clearances through the security manager and determine a "need to know" prior to allowing access to material in their container.

4.1.3. When any 305 RQS safe becomes unserviceable, the classified material contained in that safe will be transferred to another 305 RQS safe or the Intelligence Vault, 305 RQS/IN (building 1630). The safe the material is being transferred to must be approved for storage of classified to at least the level of the material being transferred. An AF Form 310, **Document Receipt and Destruction Certificate**, will be prepared by the custodian of the classified material on transfer into the courtesy storage safe.

4.1.4. If there are no 305 RQS safes available (or if directed by Davis-Monthan AFB Security Forces), classified material will be taken to 355th Wing Command Post (building 2300) for storage. The Command Post will issue a receipt for pickup.

4.2. Daily Security Inspections. Functional areas with assigned safes or secure telephone units will establish a system for end-of-day security checks. As an integral part of the security checks, Standard Forms (SF) 701, **Activity Security Checklist**, and 702, **Security Container Check Sheet**, will be used to record such checks. Individuals responsible for accomplishing daily security inspections will be identified to the security manager. Individuals will then be designated by memorandum from the security manager. The memorandum will be signed by the commander.

4.2.1. A check is required at the end of each duty day.

4.2.2. Checks are **not** required on weekends, holidays, or other nonduty days.

4.2.3. All security container openings and closings will be recorded on a SF 702. Also, at the close of business, the SF 702 must be checked off as an integral part of the security check system. In the absence of another person, the same person locking the container may also check (verify) the locking action.

4.2.4. All persons responsible for the security container will be listed on a SF 700, **Security Container Information**. The primary custodian will be the first name listed. The SF 700 and AFTO Form 36, **Security Equipment Maintenance Record**, will be maintained inside the locking drawer of each security container.

4.3. Emergency Protection. The emergency protection and removal of classified material plan will be developed by the Security Manager using AFI 31-401 guidelines. A copy of this plan will be posted on all safes.

4.3.1. General. Container custodians must know the priority assigned to the material in their container.

4.3.2. Priority. Priorities for removal and protection of classified materials are:

4.3.2.1. Priority 1. All TOP SECRET, Cryptological, or Communications Security (COMSEC) material.

4.3.2.2. Priority 2. SECRET material.

4.3.2.3. Priority 3. CONFIDENTIAL material.

4.3.3. Emergency Protection in the Event of a Fire. Security container custodians will immediately secure all classified material in their containers. The containers will be locked prior to evacuating the building.

NOTE:

At no time will classified material be left unattended.

4.3.4. Implementation. When ordered to implement emergency protection and removal of classified material, two appropriately cleared individuals (one will act as a back up should the first become incapacitated) will:

4.3.4.1. Collect and secure all classified material in classified containers. Allow no one access to the material. Stand by for evacuation and classified material relocation instructions from the commander or designated representative. At no time will classified material be left unattended.

4.3.4.2. When ordered to relocate classified material, the container custodians will immediately remove all classified material from their container and transport it to: Primary **Emergency Storage Location**--355 CS/SCCS (building 4212, COMSEC Vault); or, if the primary location is damaged or not secure **Alternate Emergency Storage Location**--Intelligence Vault, 305 RQS/ IN (building 1630).

NOTE:

Classified material will be placed in boxes, bags, waste cans, butt cans, any other usable container, or bound with wire, string, or tape to facilitate handling and prevent loss. Whatever you plan to use must be kept immediately available. If during transit, it becomes obvious that material can no longer be protected, the ranking person accompanying the material will destroy it by burning or any other means to make recognition impossible.

4.4. Transmission and Receipt of Classified Material. The security manager will supervise the preparation of all classified material for transmission.

4.4.1. Facsimile. Only authorized secure facsimile machines within the 305 RQS will be used to transmit classified information. Authorized secure facsimile machines are located in building 1630, rooms 120 and 126, and in building 1750, room 130. Also a secure facsimile machine is located at the 355th Wing Command Post.

4.4.2. Classified Couriers. Personnel tasked to act as classified information couriers will report to the security manager to receive their required briefing, inspection exemption memorandum, and courier authority memorandum. The security manager requires at least 2 working days to process the necessary courier documentation.

4.4.2.1. A memorandum from the security manager signed by the commander will designate squadron personnel as authorized classified couriers. The security manager will ensure designated personnel are thoroughly familiar with their duties and responsibilities and are briefed on the current applicable mobility plan. The 305 RQS Plans Office will be provided a courtesy copy of the memorandum for deliberate or contingency planning purposes.

4.4.2.2. DD Forms 2501, **Courier Authorization**, will be issued to authorized couriers by the security manager. When a member is no longer authorized to be a courier or leaves the unit, the DD Form 2501 will be returned to the security manager. These forms are accountable and will not be transferred to another member. The classified courier appointment memorandum will also be reaccomplished.

4.4.2.3. DD Forms 2501 expire after 1 year and re-evaluation is made by the security manager and approved by the commander annually.

4.5. Internal Handling:

4.5.1. Classified material will be stored in approved security containers located in Flight Management (DOO), building 1630, rooms 103, 120, and 126; Electronic Warfare (LGMV), building 1750, room 130; and, the Plans (XP), building 5426, room 109.

4.5.2. Classified material picked up and received during nonduty hours (i.e., weekends, holidays, etc.) will be stored in the Central Security Control (CSC) until it can be moved to one of the approved security containers. Security controllers will account for all classified material on the Security Forces Blotter.

4.5.3. Unprotected classified material will be immediately protected by the discoverer. The material will be taken to 355th Security Forces Squadron, Information Security Flight (355 SFS/SFAI) during duty hours and CSC during nonduty hours. CSC will notify SFAI via telephone if they receive unprotected classified material.

4.6. Removal of Classified Material from IN. The following procedures will be adhered to when transporting documents or media of any kind, classified or unclassified, out of the 305 RQS IN Vault. These procedures apply to all documents or media leaving the vault area whether they originated there or not.

4.6.1. If the documents or media are classified, proper justification for removal of such items must be obtained from the Chief of Intelligence or a designated representative. While outside the vault, these items must be safeguarded in accordance with directives and returned or secured as soon as possible as the situation dictates.

4.6.2. If the items are unclassified, they are to be checked by another member of the Intelligence Section before removal to ensure that classified items are not inadvertently mixed in with the unclassified. If another person is not available, the material will not be removed until a person is available. Exception: If the removal of such material is considered mission critical, it may be removed at the discretion of the person removing it. This also applies to personal or work-related satchels, briefcases, or other containers.

5. Reproduction of Classified Material. The following 305 RQS officials are designated to approve the reproduction of SECRET and CONFIDENTIAL material for which reproduction limitations and prohibitions have not been established: Commander, Deputy Commander for Operations, and Director of Intelligence.

5.1. The only unit copiers authorized for classified reproduction: DOO, Canon NP4050, serial number NCJ02331, building 1630, room 126; Weapons and Tactics (DOK), Canon Color Laser F11931, serial number CGL 02513, building 1630, room 118; and, Information Systems (SCB), Canon NP6035, serial number NGL 12198, building 5426, room 101.

5.2. A memorandum designating unit individuals authorized to reproduce CONFIDENTIAL and SECRET information will be generated by the security manager, signed by the commander, and filed in the SCB office. The memorandum will be posted immediately adjacent to the copy machines. AFVA 205-9, *Classified Reproduction Rules*, will also be posted instructing users in the proper use and clearing procedures.

5.3. Those persons authorized to copy classified will have the documents reviewed by an individual who is authorized to approve classified reproduction. The documents will be reviewed to ensure the need and quantities are valid. Reproduction of classified material will be kept to an absolute minimum and will be accomplished only on equipment specifically designated for the reproduction of classified material.

5.4. Follow instructions posted by the copier. When possible, two individuals with security clearances equal to (or higher) the level of material being reproduced will be present during the reproduction process. They will:

5.4.1. Lock the doors and cover any windows within line of sight of documents being reproduced.

5.4.2. Not allow entry of other personnel during the reproduction process.

5.4.3. Reproduce only the number of copies needed.

5.4.4. Ensure all classified material is removed from the copier by removing all copies and originals after reproduction is completed.

5.4.5. Run five blank sheets through the copier to ensure image-carrying parts are cleared after reproduction. Destroy these sheets and any bad copies as classified waste.

5.4.6. Recheck the copier and area for classified material before leaving. Check trash cans for copies inadvertently discarded; check table tops for material that may have been placed on them; check copier bins; and, check the floor and area around and behind the copier for copies that may have "floated" there.

5.4.7. Ensure reproduced classified information is marked with the proper classification markings according to AFI 31-401.

5.4.8. Protect all classified materials with the appropriate cover sheets (SF 704, **Secret Cover Sheet**, or SF 705, **Confidential Cover Sheet**).

5.5. Classified information will ONLY be processed on automatic data processing equipment (ADPE) approved for classified use by 355th Communications Squadron (355 CS).

6. Transfer of Classified Material On-Base:

6.1. TOP SECRET material will only be transferred between TOP SECRET Control Accounts by persons authorized in writing by TOP SECRET Control Officers (TSCO). Strict adherence to established written procedures will be maintained. See paragraph 7 of this instruction.

6.2. SECRET and CONFIDENTIAL material will be enclosed in an envelope, briefcase, or similar container. Attach the appropriate classified information cover sheet to the front of the material before it is placed into the container. The container will not bear any markings to indicate the contents are classified.

7. TOP SECRET Control Administrative Policies:

7.1. The TSCO and the alternate TSCO will receipt for all TOP SECRET messages and packages from the Armed Forces Courier Service (ARFCOS) when on duty. Alternate personnel can receipt for TOP SECRET message traffic when it is operationally necessary and the primary and alternate TSCOs are not present or available for duty. Personnel authorized to pick up TOP SECRET messages will be included in the Message Management Memorandum provided to the Base Communications Center by the SCB Office.

7.2. ARFCOS packages will be processed following the standards prescribed in AFI 31-401. The TSCO or alternate will examine the package for abnormal appearance. In the event of irregularities, do not open the package. Call the security forces immediately. When a COMSEC account person receipts for the package, countersign the receipt form to show a continuous receipt trail for the package.

7.3. After opening examine the contents of the package with the transmittal form (normally an AF Form 310). Sign the receipt and return it via first class mail to the originator. Notify the Commander or Deputy Commander for Operations of receipt of subject document. Prepare AF Form 143, **Top Secret Register Page**, and AF Form 144, **Top Secret Access Record and Cover Sheet**, per AFI 31-401.

7.4. Access to TOP SECRET material will be limited to those with security access requirement (SAR) coding on the current ASCAS.

7.5. If TOP SECRET material is removed from classified storage, it will be done in accordance with AFI 31-401. Primary responsibility during an emergency is to safeguard the TOP SECRET material.

7.6. The TSCO and alternate are authorized to serve as certifying officials on the AF Form 143 for the destruction and witnessing of destruction for TOP SECRET material. Both officials (i.e., destruction and witness) are required to document destruction of all TOP SECRET material. The TSCO or alternate will complete the destruction block of the AF Form 143. Any 305 RQS personnel with a TOP SECRET clearance may act as a witnessing official. Document all destruction on AF Form 143 and retain in accordance with AFMAN 37-139 and AFI 31-401.

8. Secure Telephone Unit-III (STU):

8.1. Definitions:

8.1.1. The STU Responsible Officer (SRO) is appointed by the unit commander (CC). Communication-Computer Systems (SC) is the STU-III SRO. The SRO requests crypto ignition keys (CIK) from the Key Management Center (KMC) and issues CIKs to STU users. The SRO approves and monitors STU instrument locations. The SRO conducts initial training and subse-

quent training directed by 355th Communications Squadron COMSEC Accounting Section (355 CS/SCCS).

8.1.2. Person in charge of the office where the STU is assigned.

8.2. Responsibilities. Each STU user will ensure the procedures outlined in this instruction are located next to the STU and are strictly observed. Each individual STU user will comply with the following:

8.2.1. Each STU user must call the KMC at 1-800-635-6301 once each year to update the firefly key within each STU. The user will also call the KMC once each quarter to receive an update compromise information message.

8.2.2. Each new STU user must receive initial training conducted by the unit SRO. Training will be accomplished and documented when new policies or major program changes occur.

8.2.3. When the STU is in the unkeyed mode it will only be used to place unsecure, unclassified calls. Units are unkeyed when the CIK is removed.

8.2.4. When the terminal is in the keyed mode (CIK installed in the STU), the STU must be afforded security protection commensurate with the classification level of the key. Authority to use the STU in the keyed mode will only be given by the user. The user will ensure the individual has a security clearance equal to the classification level of the CIK. The authority to use the STU will be based on a need-to-know requirement.

8.2.5. When unauthorized personnel are in the area, the keyed STU must be under the control and within view of at least one appropriately cleared and authorized person.

8.2.6. Before placing the unit to the keyed mode and initiating the secure function, the user must ensure all personnel in the area have clearances to the level of information being discussed and have a need-to-know. All other individuals must leave the area. The area will also be secured to prevent unauthorized individuals from overhearing the information.

8.2.7. Strict attention must be paid to the STU authentication display to ensure the classification level of the conversation does not exceed the highest classification displayed. Ensure the STU called does not contain an expired key scroll. This can be monitored on the display once the STU goes secure. If the STU called contains an expired key, DO NOT discuss or transmit classified information. Report the identity of the STU called to your SRO.

8.2.8. If maintenance or repair of the STU is beyond the scope of the troubleshooting described in the user manual, report this information to the SRO.

8.3. Locations:

8.3.1. 305 RQS CC's office, building 5426, room 107.

8.3.2. 305 RQS Deputy Commander for Operations (DO) office, building 1630, room 104.

8.3.3. Director of Intelligence (IN) vault, building 1630, room 120.

8.3.4. 305 RQS Deputy Commander for Maintenance (LG), building 1750, room 205.

8.3.5. 305 RQS Chief of Plans (XP) office, building 5426, room 109.

8.3.6. 305 RQS Electronic Warfare (LGMV) office, building 1750, room 130.

8.3.7. 305 RQS Weapons (LGMR) office, building 1632, room 107.

8.3.8. 305 RQS Communications Element (SCS), building 1630, room 131.

8.4. Key Control:

8.4.1. STUs not operational 24 hours a day will have the CIK removed at the close of business. The CIK must be an item on the end-of-day security checklist.

8.4.2. Once removed, the CIK will be stored in a GSA-approved container in the same or different room. If a GSA-approved container is not available, the room must have a locked door and additionally, the CIK will be stored in a locked cabinet, desk, file cabinet, etc. The adequacy of storage alternatives for the CIK should be determined on a case-by-case basis with your SRO.

8.4.3. If you lose your CIK, you must notify your SRO within 72 hours.

8.4.4. If the STU is to be shipped to a temporary duty location, the CIK will be shipped separately from the STU instrument or hand-carried by the user or a classified courier. While in use at the TDY location, the same home-station policies on control, use, and protection apply.

8.5. Reportable Incidents:

8.5.1. CIKs left in STU instrument after the end of the business day. Exceptions: 24-hour work areas and areas approved for open storage.

8.5.2. Lost STU instruments, seeded, or operational keys.

8.5.3. Personnel not authorized or cleared by user making secure calls on STUs.

8.5.4. Secure calls completed using an expired key by either the initiator or recipient.

8.5.5. Any instance where the authentication information displayed during a secure call is not representative of the terminal called.

8.5.6. Failure to adequately protect or to erase CIK associated with a lost terminal.

8.5.7. Any instances where the display indicates terminal called contains a compromised key.

8.5.8. CIK inserted in a STU left unattended or with no authorized user present.

8.5.9. Any instance where the display is inoperative and a secure call is made.

8.6. Emergency Procedures. In case of a fire, natural disaster, or covert threat, the following action will be attempted, time and situation permitting. Attempt to remove the CIK and secure it in a GSA-approved container or retain it in your possession until it can be turned over to the SRO.

KENT D. CLARK, Col, USAFR
Commander

Attachment 1**SECURE BRIEFING CHECKLIST**

A1.1. Attendees must have a security clearance equal or higher to the level of classified being presented. Must be validated by a locally-generated Automated Security Clearance Access System (ASCAS) product (Entry Authorization List - EAL) obtained from the unit security manager. (And, by memorandums from local unit security managers vouching for attendees. Must include name, rank, SSN, and clearance.)

A1.2. Radios, beepers, and all electronic equipment capable of transmitting will be disabled, turned off, or left outside the room.

A1.3. Facility will be secured with a guard posted outside the door. If briefing is in a secure area, no guard is required.

A1.4. Windows must be covered.

A1.5. Phones must be disconnected from wall jacks.

A1.6. The taking of notes will only be authorized by the individual having custodial responsibility of the material.