BY ORDER OF THE COMMANDER
307TH RED HORSE SQUADRON

307TH RED HORSE SQUADRON
INSTRUCTION 33-201

5 MAY 2005

Communications and Information

UNIT COMMUNICATION SECURITY PROGRAM

COMPLIANCE WITH THIS PUBLICATION IS MANDATORY

NOTICE: This publication is available digitally on the AFDPO WWW site at: **http://www.e-publishing.af.mil.**

OPR: 307 RHS/CO (MSgt Joaquin Ramirez)

Certified by: 307 RHS/CC
(Lt Col Elwin A. Rozyskie)
Pages: 10
Distribution: F

This instruction implements Air Force Policy Directive (AFPD) 33-2*, Information Protection*. It describes the methods and processes, in accordance with (IAW) Air Force Instruction (AFI) 33-211, *Communications Security (COMSEC) User Requirements*, for the handling, control and use of COMSEC material. It applies only to personnel assigned to the 307th Red Horse Squadron (307 RHS), Lackland Air Force Base Texas.

This is the initial publication of 307th Red Horse Squadron Instruction 33-201.

1. Responsibility. Protection of COMSEC material is the responsibility of COMSEC Responsible Officer (CRO), alternate CRO and users. To include those that originate, process, store, receive or dispatch.

2. Taskings.

2.1. CROs will notify the COMSEC manager, in writing, of any new requirements, changes, or pending requirements to existing requirements.

2.2. Annually review the requirement for COMSEC material.

2.3. Ensure individuals granted access to COMSEC materials have a final security clearance equal to or greater than the classification level of the COMSEC material accessed and have a need-to-know.

2.4. Maintain an accurate list of personnel with authorized access to COMSEC holdings.

2.5. Conduct initial and refresher training of all COMSEC users.

2.6. Ensure responsibility for receiving, accounting for, checking pages of, handling, using, and safeguarding all COMSEC material that they or their alternate receives until it is destroyed or returned to the COMSEC account.

2.7. Develop local operating instructions.

2.8. Perform inventories.

2.9. Verify COMSEC materials are inventoried according to their respective accounting legend codes.

2.10. Carry out duties as deemed necessary by the COMSEC manager.

2.11. Issue COMSEC materials to users.

2.12. Issue a receipt to in-transit personnel who turn-in material for safekeeping.

2.13. Return or destroy all material as the COMSEC manager directs.

2.14. Keep all records according to Air Force Records Information Management System (AFRIMS) Records Disposition Schedule (RDS).

2.15. Develop an emergency action plan (EAP).

2.16. Ensure required security checks are performed.

2.17. Provide an update report every 30 days on findings identified during assessments and audits.

2.18. Report all known or suspected COMSEC deviations to the COMSEC manager.

2.19. Enroll all applicable personnel in the Cryptographic Access Program (CAP) and remove them from the CAP when they are removed from the access list.

2.20. Obtain relief of accountability from the COMSEC manager prior to leaving their current duty assignment. Ensure all COMSEC material is returned to the COMSEC manager and signed over to the new CRO.

2.21. Obtain new COMSEC equipment according to AFI 33-103*, Requirements Development and Processing.*

2.22. Alternate CRO will take the place of and provide continuity for COMSEC material in the absence of the CRO.

2.23. COMSEC users have access to COMSEC material and also the responsibility for safeguarding them. COMSEC users must ensure that anyone who receives COMSEC material had authorization and has verified the individual's security clearance. Users must follow all security rules at all times. Report to the CRO or the COMSEC manager any circumstances, intentional or inadvertent acts, which could lead to the unauthorized disclosure or classified information, including its loss, improper use, unauthorized viewing, or any other instance that could possibly jeopardize the value of COMSEC material.

2.24. Safeguard COMSEC material according to AFI 33-211 and control the material locally until destroyed or turned-in.

2.25. Return material to the CRO on request.

2.26. Maintain and familiarize themselves with correct procedures for operating associated cryptographic equipment and devices utilizing applicable Air Force Systems Security Instructions (AFSSI), Air Force Kryptologic Aids Operations (AFKAO), Kryptologic Aids Operations (KAO), or instructions provided by the CRO.

2.27. Report immediately any known or suspected compromise of COMSEC material to the CRO or COMSEC manager.

2.28. Be trained by the CRO prior to being granted unescorted access to COMSEC materials.

2.29. Obtain relief of accountability from the CRO prior to being relieved of duties as a COMSEC user.

3. Requirements.

3.1. Appointment Memorandum.

3.1.1. The Unit Commander will appoint CROs, in writing, a primary and alternate to receive material from the COMSEC account 626506 building 9225 and 3757 IAW AFI 33-211, Attachment 2. The memorandum must include each individual's name, rank, social security number, security clearance, duty telephone, and locations the individuals may carry COMSEC materials to and from. Update this letter annually or as changes occur. Maintain the current Primary and Alternate CRO appointments. CROs will be changed if pending a transfer or will be on temporary duty for more than 90 days**.**

3.2. COMSEC Requirements Memorandum.

3.2.1. Notify the COMSEC manager, in writing, of any new requirements, changes, increase or decrease or pending requirements to existing requirements, COMSEC Requirements memorandum IAW AFI 33-211, Attachment 3. Include the equipment being used for each Short Title require. All COMSEC equipment must be included on the Requirements memorandum, and proof that the equipment has been added to a base supply account must be submitted to the COMSEC account IAW AFI 33-211, Attachment 3. The requirement for COMSEC materials must be reviewed and submitted annually along with a current copy of the Custody Account/Custody Receipt Listing (CA/CRL) showing the equipment listed. The CRO will submit a letter to the COMSEC Manager requesting the COMSEC materials that are required to support the mission. Update the letter when there are new requirements or changes (increase or decrease) to existing requirements.

3.3. COMSEC Access List.

3.3.1. Limit access to COMSEC material in the facility to individuals named on an officially published access list (AFI 33-211, Attachment 4). The list must contain the names, rank, full social security number, and security clearance of all individuals who have COMSEC responsibilities in the facility. All personnel on the list must have a final clearance equal to or higher than the COMSEC information to which they have access. Identify individuals on the authorized access list who may authorize other to a minimum. The list must be reviewed annually by the CRO for continuing need for access security clearance. Unless other individuals are specifically authorized by the COMSEC manager, only the base COMSEC manager's staff and all individuals listed on the access list are authorized access to COMSEC material and COMSEC users' records. Do not allow access to other inspection, periodic review, and staff assistance personal without prior approval from the Headquarters Air Force Material Command (HQ AFMC) COMSEC (CSO/SCSS).

3.4. COMSEC EAPs.

3.4.1. The CRO will develop an EAP that consists of task cards that have been coordinated with the COMSEC manager for review and endorsement. The EAPs specify the actions to be taken during Fire, Natural Disaster, and Bomb Threat evacuations. The EAPs are located in the Logistic Plans office, building 3758. All personnel who have access to COMSEC must participate in the conduct, document reviews and EAP training exercises (dry runs) at least semi-annually. This ensures that all individuals can effectively carry out their emergency duties.

3.5. Storage.

3.5.1. All COMSEC materials will be stored in a General Services Administration (GSA) approved Class 6 or better container. Combinations will be given to those who are authorized by the CRO, and all individuals having combinations to COMSEC safes must be on the published access list. The safe combinations must be changed at least once a year or every six months if North Atlantic Treaty Organization (NATO) material is maintained, when an individual leaves who has access to COMSEC material, when combination is compromised, or when personnel are removed from access list.

3.6. Air Force COMSEC (AFCOMSEC) Form 16, **COMSEC Account Daily Shift Inventory**.

3.6.1. Inventory of the COMSEC material shall occur each day the safe is opened. Inventory must be completed just prior to locking the safe for the final time each day. Use only "black" ink to make entries on the inventory (AFCOMSEC Form 16). Annotate each block by using an "X" and individual's initial on the bottom of the form. Do not use check marks or slashes (/). Do not use "whiteout", correction tape, or erasures. If an error is made, neatly draw a single line through the error, initial, and number the error in the margin next to the error. Record explanatory remarks on the back of the form include the error number, date discrepancy was discovered and corrected, detailed description of the discrepancy, and the initial of the individual who made the correction. When receiving, returning, or destroying COMSEC material annotate the AFCOMSEC Form 16. With the AFCOMSEC Form 16 you are keeping track of the materials held. A new AFCOMSEC Form 16 must be completed each month. On it you shall list all COMSEC material held. The CRO must review inventories monthly to make sure they are accomplished correctly.

3.6.2. Document the review by initialing and dating the bottom corner of AFCOMSEC Form 16. Keep the current and the previous six months of inventory records on file. Limit access to these records and files to those individuals who manage, administer, operate and maintain COMSEC aids and equipment. During record maintenance and administrative staff assistance visits and program management review, the reviewers may only check the AFRIMS File Maintenance and Disposition Plan. Do not grant reviewers access to COMSEC materials, records, or file.

3.7. AF Information Management Tool (IMT) 1109, **Visitors Register Log**.

3.7.1. Only the Base COMSEC Account personnel who have been designated, in writing, and individuals named on the Access List are authorized to view our COMSEC. All others must have permission from the Base COMSEC office. A new AF IMT 1109 must be completed each month. On it list the date, name, grade, organization and signature of escort for each visitor, including time in and time out. Only individuals who are so designated on the Access List may sign-in and escort visitors. All visitors must present a picture identification. All visitors must be escorted at all times while working around COMSEC materials. Visitors must never be left alone with access to COMSEC materials. Each AF IMT 1109 shall remain on file current plus one year after date of last visitor recorded on the form.

3.8. Standard Form (SF) 700, **Security Container Information Form**.

3.8.1. It is required the SF 700 be used to record combination change. The combination must be changed when anyone having the combination of a safe is relieved of duty for any reason, a combination is compromised, or any repair work on combination lock. It is mandatory that the combination be changed at least once a year. To accomplish the changing of combination, refer to the instruction for the lock. A SF 700 record of combination change shall be completed. Attach the top copy of SF 700 to the inside locking drawer of the safe. Detach Copy 2A from Envelope 2. Stamp the envelope with the highest level of classification of COMSEC material in container (Account Legend Code 1).

3.9. SF 701, **Activity Security Checklist**.

3.9.1. A required security check will be made each workday to ensure proper storage and safety of all classified COMSEC material by the area checker for each workday. The immediate area will be checked for unsecured COMSEC materials. The safe's "opening handle pulled and verified" to assure the safe is properly locked. Initial the form each workday showing the safe has been checked. A new form will be started each month and the previous form destroyed.

3.10. SF 702, **Security Container Check Sheet**.

3.10.1. Only those personnel authorized access to the safe shall have the combination. The opening of the container will be documented using an SF 702. Also, locking the safe shall be documented by the SF 702. After locking the safe, it will be checked by another individual who will annotate the "checked by" block. On the days the safe is not opened, and personnel are present in the area, the SF 702 must be annotated with time and initialed by the person performing the end of day security check. Prepare new form each month (or as needed if completely used during any month) per AFI 33-211. Destroy the previous month's form.

3.11. Air Force Technical Order (AFTO) IMT 36, **Maintenance Record for Security Type Equipment**.

3.11.1. An AFTO IMT 36 must be kept to provide a historical maintenance record for the safe. Authorized maintenance personnel will make a record of each inspection and type of maintenance made. This IMT will be kept inside the safe's locking drawer. The date of combination changes is not recorded on AFTO IMT 36. Qualified personnel shall do preventive maintenance and inspection requirements every five years. Reference Technical Order (T.O.) 00-20F-2, *Inspection and Preventive Maintenance Procedures for Classified Storage Containers*, for additional information.

3.12. SF 153, **COMSEC Material Report.**

3.12.1. All items must be accounted for from date of receipt until date of destruction or when returned to the COMSEC account. Maintain a copy of the SF 153 of the COMSEC material signed for or the destruction record.

4. Training and Required Readings.

4.1. Initial Training/Annual Refresher Training.

4.1.1. All personnel with access to COMSEC material must complete initial training. Initial training will be conducted using the outline in AFI 33-211. (Initial training/annual refresher training both the primary CRO and alternate CROs (ACRO) must be accomplished by COMSEC Account Personnel.) CRO/ACRO initial, as well as, annual refresher training must be documented on an AF IMT 4168, **COMSEC Responsible Officer and User Training Checklist**, initialed, signed and dated by the base COMSEC. Once this has been documented, it will remain on file for one year or if the individual is relieved of duty during that year. (CRO or ACRO is then responsible for training anyone else they authorize to access their COMSEC material.)

4.1.2. Complete COMSEC Responsible Officer training.

4.1.3. Read AFI 33-211.

4.1.4. Read AFI 33-211/AFMC Sup 1.

4.1.5. Read the 307 RHS COMSEC OI.

4.1.6. Read any applicable KAO, Kryptographic Aids Manual (KAM), and AFSSI for your equipment. Review all of the COMSEC EAP task cards.

4.1.6.1. Once completed, each individual must sign and date certification IMT (AF IMT 4168, located: **https:www.e-publishing.af.mil**) to document completion of the above training.

4.1.6.2. CRO maintains only the most current AF IMT 4168 on file. (AFI 33-211, para 5.)

4.1.6.3. Location: COMSEC continuity binder, building 3757, room 3.

4.1.6.4. Subject to two inspections: COMSEC office (semi-annual) Information Assurance Assessment Program (IAAP) (every two years).

4.1.6.5. Inspectors will compare COMSEC training documentation against COMSEC access list to determine if required training is being accomplished.

4.2. Semi-annual Training. All personnel having unescorted access to COMSEC material must complete and document the following:

4.2.1. Read 307 RHSI 33-201.

4.2.2. Read each applicable KAO, KAM, or AFSSI for your equipment.

4.2.3. Read AFI 33-211.

4.2.4. Demonstrate performance of EAPs, rotating through all EAPs, completing a different one every six months by utilizing a real world situation like a bomb threat, fire drill, etc., or performing a dry run (walking through of the steps) of EAPs as if it was a real world situation.

4.3. Once training is completed, training must be documented on a memorandum detailing the following: scenario, date, names, and signatures of each trainee, and trainer. (Use example in CRO continuity binder, tab B to document this training.)

4.3.1. Subject to three inspections.

4.3.2. Self-Inspection (semi-annual, just before COMSEC office).

4.3.3. COMSEC office (semi-annual).

4.3.4. IAAP (every two years).

4.3.5. Inspectors will compare COMSEC training documentation against COMSEC access list to determine if required training is being accomplished.

5. Page Checks of Classified Communications Security Publications.

5.1. To protect the integrity of COMSEC aids, check pages of classified COMSEC publications:

5.1.1. When receiving single copies of editions of material from the COMSEC account and you cannot get a replacement copy sufficiently before effective period. Check that the document does not have printing or productions errors. Report errors to the COMSEC manager. Page checks of classified documents are also required annually.

5.1.2. After a change adds, deletes, or replace pages or affect page numbers. ***NOTE:*** A person other than the one making the change must do the page check.

5.1.3. The COMSEC manager and CRO must ensure completed page check of COMSEC publications. Unclassified documents do not require page checks unless page change value amendments are made to them.

5.1.4. Verify that all pages are current and present by comparing the list of effective pages (typically on of the last few pages) against the actual pages in the document. Check to see that each page is exactly as described. Record the check on the record of page checks page, or, if the publication has no record or page checks, on the record of amendments page or front cover. Report any discrepancy immediately to the COMSEC manager.

6. Pick-Up and Hand Receipting for COMSEC Material.

6.1. The CRO or a trained, cleared alternate will pick up new COMSEC material at the Base COMSEC. The Base COMSEC account will be given a SF 153. This form will list the following:

6.1.1. Short title

6.1.2. Edition

6.1.3. Quantity

6.1.4. Publication number

6.1.5. Legend code

6.1.6. Verify the information on the hand receipt with the material. If all is correct, sign and date the SF 153. You will be given a copy of the SF 153 and you must return directly with the material and the SF 153. Upon return, add the material to the inventory and store it in the safe. File the SF 153. Only the current SF 153 will remain on file.

6.1.7. If the CRO or an alternate with an active hand receipt on file for COMSEC material is relieved from duty, he or she must be relieved from accountability for the material signed for. To accomplish this, contact the Base COMSEC, Defense Switched Network (DSN) 473-2436, and inform them of the individual's reassignment. The Base COMSEC will reaccomplish all active hand receipts for that individual. A current CRO or alternate shall sign the new hand receipts. See CRO continuity binder, tab 4 for an example of the SF 153. When the COMSEC manager directs, destroy the material, record destruction of classified documents on an SF 153, and keep the destruction certificate for 3 years IAW AFI 33-211.

7. Routine Destruction.

7.1. The authorized method for routinely destroying paper COMSEC aids are using a National Security Agency authorized high security shredder or burning. Unless a waiver is on file, routine destruction of COMSEC material must be completed no later than 12 hours after supersession. However, routine destruction will take place the first duty day following a weekend or a holiday. Two appropriately trained and cleared individuals, a destruction official and a witnessing official, must destroy the material. All destruction of key tapes shall be accomplished using an approved GSA shredder (KD-100) located in the Logistics Plans office bldg 3758, or by taking the material to the COMSEC account in building 9225, 37 CS/SCBS, or burning.

7.2. Keytape Segments. The destruction of individual keytape segments will be documented by annotating the disposition form contained with the keytape canister. The initials of destruction and witnessing officials and date of destruction shall be annotated on the disposition record. This Disposition Record Card will be kept for 3 years with the destruction report.

7.3. When burning paper COMSEC aids, the fire must reduce all material to white ash. Be sure no burned pieces escape, inspect ashes and, if necessary, break up or reduce them to sludge. Do not place keying material in bags for destruction with other classified waste.

7.4. Since our facility does not normally operate on weekends, a request for a 24-hour extension is on file. However, routine destruction will take place the first duty day following the weekend. Two appropriately trained and cleared individuals, a destruction official and a witnessing official, must destroy the material. All destruction of key tapes shall be accomplished using an approved NSA shredder located in building 3758 Logistics Plans office, or burning.

8. Daily Operations.

8.1. The Safe. A GSA Class 6 or better safe must be used to store COMSEC. Only those personnel authorized access to the safe shall have the combination. The opening of the safe will be documented with the use of an SF 702. Also, locking the safe shall be documented by the SF 702. After locking the safe, it will be checked by another individual who will annotate the “checked by” block on the SF 702. If no other person is available, the individual locking the safe shall annotate the “checked by” block. On the days the safe is not opened, the SF 702 must include the time and initials of the individual performing the end of day security check. See CRO continuity binder in building 3757, room 3, tab 4 for example of an SF 702.

8.2. When anyone having the combination of the safe is relieved of duty for any reason, and at least once a year, every six months if you hold NATO material, the combination must be changed. To accomplish this, refer to the instructions for the lock. An SF 700, record of combination change, shall be completed. Place the top copy on the inside locking drawer of the safe. See CRO continuity binder for example of SF 700.

8.3. The highest level of classified information authorized to be stored in the safe must be displayed in an easily visible location. Ensure a sticker with the following information is placed on the inside lip of the locking drawer: HIGHEST AUTHORIZED CLASSIFICATION IS: (*INPUT CLASSIFICATION HERE*)

8.3.1. An AFTO IMT 36 must be filled out and maintained for each safe. Keep this IMT in the locking drawer. Do not put safe combination changes on this form, only maintenance items. This IMT is also used to indicate a physical inspection of the container was performed by a certified locksmith, and the container recertified as GSA Class 6 (or better) at least once every five years.

8.4. Unescorted Access. Unescorted access to COMSEC material is limited to those individuals listed on the COMSEC access list posted on the safe. This list will be updated annually, or as required.

8.5. Escorted Access. Individuals on the access list and marked with an asterisk (*) by their name are authorized to grant access to those, not listed, with a valid need to know and proper security clearance. Those granted access must be signed in on an AF IMT 1109 and escorted until they leave the area. AF IMT 1109 shall remain on file for one year from the date of last entry. See CRO continuity binder for example of AF IMT 1109.

8.6. End-of-day Security Check. The safe shall be checked “opening handle pulled and verified” and the security checklist SF 701 appropriately annotated by the individual responsible for closing the area.

9. Reporting Insecurities.

9.1. Any COMSEC insecurity shall be reported promptly to the COMSEC manager, DSN 473-2436 and one of the following individuals: JOAQUIN RAMIREZ, CRO, 307 RHS/COOF, DSN 945-6052, extension 213; or LENNY CLARK, Alternate CRO, 307 RHS/LGX, DSN 945-6052, extension 252.

9.2. The importance of immediately reporting all known or suspected physical, personnel, and cryptographic incidents can not be over emphasized. The CRO and COMSEC manager must ensure, before issuing material or equipment that users are fully aware that reports of know, suspected, or possible incidents must be reports of known, suspected, or possible incidents must be reports of known, suspected, or possible incidents must be reports immediately upon detection. Do not discuss specifics of the incidents over a non secure phone. Just inform the party that there is a problem, and you need to talk about it in person.

10. Adopted Forms/IMTs. AF IMT 1109, **Visitors Register Log**; AF IMT 4168, AFCOMSEC Form 16, **COMSEC Account Daily Shift Inventory;** AFTO IMT 36, **Maintenance Record for Security Type Equipment;** SF 153, **COMSEC Material Report**; SF 700, **Security Container Information Form;** SF 701, **Activity Security Checklist**; and SF 702, **Security Container Check Sheet**.

ELWIN A. ROZYSKIE, Lt Col, USAFR
Commander

Attachment 1

GLOSSARY OF REFERENCES AND SUPPORTING INFORMATION

References

AFI 33-103, *Requirements Development and Processing*

AFPD 33-2, *Information Protection*

AFI 33-211, *Communications Security (COMSEC) User Requirements*

T.O. 00-20F-2, *Inspection and Preventive Maintenance Procedures for Classified Storage Containers*

Abbreviations and Acronyms

ACRO— alternate CRO

AFI— Air Force instruction

AFRIMS RDS— Air Force Records Information Management System Records Disposition Schedule

AFSSI—Air Force Systems Security Instructions

AFTO— Air Force technical order

AFKAO—Air Force Kryptologic Aids Operations

CA/CRL— Custody Account/Custody Receipt Listing

CAP— Cryptographic Access Program

COMSEC— Communications Security

CRO— COMSEC responsible officer

DRC—Disposition Record Card

DSN— Defense Switched Network

EAP— emergency action plan

GSA— General Services Administration

HQ AFMC— headquarters Air Force Material Command

KAM— Kyptologic Aids Manual

KAO—Kryptologic Aids Operations

NATO—North Atlantic Treaty Organization

IAAP— Information Assurance Assessment Program

IAW— in accordance with

IMT— information management tool

SF— standard form

T.O.— technical order