

Communications and Information

Communications Security (COMSEC) Operations

COMPLIANCE WITH THIS PUBLICATION IS MANDATORY

NOTICE: This publication is available digitally on the Headquarters LA ANG WWW site at:
<https://hq.mil>

OPR: 159CF/SCBS (MSgt Tiffanni L. Beckham) Certified by: 159CF/SCB (CMSgt Elaine P. Vix)

Pages: 14

Distribution: F

This instruction implements CMS 21A, *Communications Security Material System Policy and Procedures for Navy Electronic Key Management System Tiers 2 & 3* and AFI 33-211, *Communications Security (COMSEC) User Requirements*. It outlines responsibilities and clarifies procedures to properly handle COMSEC material issued by the 159th Fighter Wing (FW) COMSEC Custodian. This instruction applies to all COMSEC users who receive COMSEC material from the 159FW COMSEC account.

1. Glossary of References and Supporting Information. See Attachment 1.

2. Introduction. This instruction sets forth procedures for all COMSEC users. It describes COMSEC duties and the minimum requirements for issuing, safeguarding, controlling, and disposing of COMSEC material. It also applies cryptographic and physical security measures to COMSEC material and facilities. Persons involved in the handling of COMSEC material must be aware that non-compliance or deviation from the prescribed procedures can jeopardize the national security and could result in prosecution of the parties concerned under espionage laws, Title 18, U.S.C., Sections 793, 794, and 798.

3. Objective. This instruction provides users with detailed procedures for the safe handling of COMSEC material, proper physical security procedures, education and training.

4. Communications Security Responsibilities.

4.1. Wing Commander. The wing commander will appoint a primary and alternate FW COMSEC Custodian.

4.2. Unit Commander. The commander of each unit that needs COMSEC material:

4.2.1. Appoints in writing a primary and at least one alternate COMSEC Responsible Officer (CRO) to receive COMSEC material (See Attachment 2).

4.2.2. May appoint more than one CRO in large units, depending on the number of COMSEC users and the volume of the material handled.

4.2.3. Takes immediate, corrective action in response to discrepancies identified during a semiannual inspection.

4.2.4. Make sure adequate, approved security containers or facilities are available for storing COMSEC material.

4.2.5. Makes sure a National Security Agency approved destruction device is readily available.

4.3. **159FW COMSEC Custodian.** The FW COMSEC Custodian:

4.3.1. Receives and issues all COMSEC materials intended for issue to the CRO via Standard Form 153, **COMSEC Material Report**, and instructs CROs in writing, how to use, control and store the material.

4.3.2. Provides guidance on setting up CRO functions.

4.3.3. Gives CROs information on effective and suppression dates, compromise information, and physical security requirements for operational systems before issuing COMSEC material.

4.3.4. Ensures all CROs receive training using all applicable guidance and publications to set up an effective training program.

4.3.5. Conducts Staff Assistance Visits semi-annually on all CRO accounts.

4.3.6. Provides written guidance concerning handling, accountability and disposition of COMSEC material to all CRO's.

4.3.7. Sets up a comprehensive training program to make sure all CRO's know how to receive, issue, safeguard and destroy the material issued to them. Training should be documented on the AFCOMSEC Form 30, **COMSEC Responsible Officer and User Training Checklist**.

4.3.8. Develops an Emergency Action Plan (EAP) to protect material held by the FW COMSEC Custodian account. Training exercises should be conducted annually to ensure proper execution of the plan.

4.4. **CROs.** Unit CRO's will:

4.4.1. Notify the COMSEC custodian, in writing, of any new requirements or changes (increase or decrease) to existing requirements as soon as the requirement is identified.

4.4.2. Review annual requirements for COMSEC material, assessing the validity of each item, and provide the COMSEC custodian in writing, the complete list of COMSEC requirements to include the quantity, purpose, and authority for each item.

4.4.3. Keep an accurate list of all unit personnel with authorized access to COMSEC materials (See Attachment 3).

4.4.4. Ensure that the FW COMSEC Custodian receives copies of all Communications Security Material Systems (CMS) User Acknowledgement Forms.

4.4.5. Make sure all persons granted access to COMSEC material have the proper clearance and a valid need-to-know, and have completed a CMS User Acknowledgement Form (See Attachment 4).

4.4.6. Set up a comprehensive, periodic training program to make sure all unit personnel with authorized access know how to handle, control and use the material. Ensure all personnel are familiar with correct procedures in operating associated cryptographic equipment. Training should be documented on the AFCOMSEC Form 30.

4.4.7. Take responsibility for receiving, accounting for, page checking, handling, using, and safeguarding all COMSEC material they receive until it is destroyed or returned to the COMSEC custodian.

4.4.8. Develop a local operating instruction (OI) on handling, controlling, and protecting COMSEC assets, including inventory, two-person integrity (if applicable), destruction, COMSEC incident reporting, secure telephone units (STU III), secure telephone equipment (STE).

4.4.9. Develop an emergency action plan for COMSEC material held by the unit and coordinate it with the FW COMSEC custodian. Training exercises should be conducted annually to ensure proper execution of the plan.

4.4.10. Report immediately to the FW COMSEC Custodian any known or suspected insecure practice or COMSEC incident.

4.4.11. Maintain and update when necessary, all instructions, messages and correspondence issued by the FW COMSEC Custodian.

4.4.12. Research all unit COMSEC requirements prior to submitting requests to the FW COMSEC Custodian.

4.5. COMSEC Users. COMSEC users have access to COMSEC materials and the responsibility for safeguarding them. COMSEC's ultimate success or failure rests with the material's individual users. The careless user or the user who fails to follow procedures for using, safeguarding, and destroying COMSEC material wastes all security efforts. COMSEC users must make sure that anyone who receives materials has proper authorization. Users must follow all security rules at all times and report to the CRO or the COMSEC custodian any circumstances or intentional or inadvertent acts that could lead to disclosure of classified information, including its loss, improper use, unauthorized viewing, or any other instance that could possibly jeopardize the value of COMSEC material. COMSEC users:

4.5.1. Safeguard COMSEC material according to all applicable guidance and control the material locally until they destroy it or turn it in.

4.5.2. Return material to the CRO upon request.

4.5.3. Familiarize themselves with correct procedures for operating associated cryptographic equipment and devices.

4.5.4. Report immediately any known or suspected compromise of COMSEC material to the CRO or FW COMSEC custodian.

5. Requesting CMS Material. CROs inform the FW COMSEC Custodian, by letter, what COMSEC material is needed (See Attachment 5). It is not the responsibility of the FW COMSEC custodian to research a customer's COMSEC requirements. CROs are required to research the requirement and provide the short title, quantity and justification to the FW COMSEC Custodian in writing in order to facilitate a request.

5.1. All requests should be submitted 60 days prior to the date that it is needed. When circumstances arise where this suspense cannot be met, the CRO will submit the request as an emergency requisition as soon as possible with the understanding that the material may not be available prior to the deployment.

5.2. All request letters must contain the short title of the material, quantity needed, and justification. Letters void of this information will be returned to the CRO for corrective action.

6. Routine Issue of COMSEC Material. All COMSEC material designated for a particular unit will be issued to either the primary or alternate CRO. Only when the CROs are unavailable will the material be issued to an authorized user assigned to the unit. This individual must have a CMS Responsibility Acknowledgement Form on file with the COMSEC custodian.

7. Routine Destruction of COMSEC Material. To safeguard encrypted traffic and U.S. COMSEC operations, destroy superceded or obsolete COMSEC material as soon as possible after the materials have served their purpose so it is impossible to reconstruct them. Superceded keying material is extremely sensitive because its compromise potentially compromises all traffic encrypted with it as well. Be very careful not to accidentally destroy COMSEC material. A destruction official must actually destroy the material. The destruction official and the witnessing official must sign destruction reports, subject to the following rules:

7.1. The destruction official is an appropriately cleared, responsible individual.

7.2. The witnessing official must have a clearance consistent with the material being destroyed.

7.3. The destruction official and the witnessing official must not sign the destruction report until destruction is complete and they have checked the destruction machine and area.

8. Page Checks of Classified COMSEC Publications. To protect the integrity of COMSEC aides pages checks of classified COMSEC publications must be accomplished:

8.1. Upon receipt from the FW COMSEC Custodian.

8.2. Before initial issue to any aircrew.

8.3. When single copies of editions of material from the COMSEC account are received and a replacement copy cannot be received before the effective period.

8.4. After a change adds, deletes, or replaces pages or affects page numbers.

8.5. Prior to destruction.

9. Routine Destruction Methods. The authorized methods for routinely destroying paper COMSEC material are burning, pulverizing or chopping, crosscut shredding, and pulping. *Note:* Crosscut shredders must reduce the residue to shreds no more than 3/64 -inch (1.2mm) by 1/2-inch (13mm) or 1/35-inch (0.73mm) by 7/8-inch (22.2mm).

10. Reproducing COMSEC Material. The reproduction of COMSEC material will be controlled by the Navy Electronic Key Management System (EKMS) Manager only. The FW COMSEC Custodians and CROs are not authorized to reproduce COMSEC material at any time or under any circumstances. Reproducing this material constitutes a COMSEC incident and will result in disciplinary action.

11. Storing COMSEC Information & Material. "Storage" as used here means using security containers, vaults, alarms, guards, etc., to protect classified COMSEC information and material during non-working hours or when authorized personnel do not directly and continuously control it.

11.1. **COMSEC Material.** All users who have classified COMSEC material must have immediate access to an authorized storage container to secure the material in case of area evacuation.

11.2. **Cryptographic Equipment and Components.** When classified equipment and components are not installed in an operational configuration, store them in the most secure storage available. As a minimum, store it as required for non-COMSEC material of the same classification. When no authorized person keeps or continuously watches unclassified cryptographic equipment, protect it by:

11.2.1. Storing unclassified equipment to prevent any unreasonable chance of theft, sabotage, tampering, or unauthorized access.

11.2.2. Not storing cryptographic equipment or fill devices (KYK-13's or KYK 15's) in a keyed condition. When necessary to store it in a keyed condition, protect it at the same level as the key it contains and place it in the COMSEC inventory.

11.2.3. Storing unkeyed Controlled Cryptographic Items in a secured facility so that in the unit commander's judgment, there is no reasonable chance of theft, sabotage, tampering or unauthorized access. When keyed, protect such equipment to prevent its unauthorized use or extraction of its key.

12. Physical Security Requirements. Areas where COMSEC material is used must meet the storage and other physical requirements for the particular classification level of the COMSEC material (see DODR5200-1WC1-2, *Information Security Program* and AFI 31-401, *Information Security Program Management*). Additional information regarding the Information Security Program can be obtained from 159th Security Forces Squadron personnel.

13. Access Controls and Procedures. CROs must only give persons with appropriate clearance and the need-to-know access to COMSEC material.

13.1. Set up controls to deny unauthorized persons access.

13.2. Limit unrestricted access to COMSEC material in a user facility to persons named on an officially published access list (See Attachment 3). The list must contain the names and clearance levels of all persons who have COMSEC responsibilities in the facility, and should include the unit commander and supervisors. All personnel on the list must have a clearance equal to or higher than the COMSEC information to which they have access.

13.3. Facilities with the locked door system must challenge and identify persons before entrance is granted. Regardless of the control system, entry procedures must identify persons seeking entry so they cannot view COMSEC activities before entering.

13.4. Record the arrival and departure of all persons not named on the authorized access list, using AF Form 1109, **Visitor Register Log**. Keep the current plus the previous 3 months of AF Form 1109 on file.

14. Safe Combinations. Lock combinations shall be classified and safeguarded the same as the highest classification of the material being protected by the combination. It is specifically prohibited for an individual to record and carry, or store insecurely for personal convenience, the combinations to COMSEC facilities or containers. Also, do not store records of combinations in electronic form in a computer, calculator, or similar device. Change the combinations of security containers used for classified COMSEC material storage:

- 14.1. At least once a year.
- 14.2. When a person who knows combinations no longer has access to the containers for any reason other than death.
- 14.3. When a container certified as locked is found open.
- 14.4. When the combination is compromised.

15. Operating Instructions (OI). Each CRO must write a COMSEC OI and coordinate it with the FW COMSEC Custodian. The OI will contain provisions for securely conducting COMSEC operations and for safeguarding COMSEC material. The procedures and instructions in the OI are specific to the user's activity. They should include procedures for cryptographic operations, local accountability for COMSEC material, COMSEC maintenance support, access restriction, storage, routine and emergency destruction, incident reporting, and procedures for relieving people who have received COMSEC material from accountability when they have been reassigned.

16. Emergency Action Plans. Each unit issued COMSEC material must understand that emergencies could expose its classified COMSEC material to loss or compromise. Planning can prevent or reduce loss or compromise and help facilities cope with two types of emergencies: accidental and hostile.

- 16.1. Activities that hold classified Accounting Legend Code (ALC) ALC-1 or ALC-2 material must develop and maintain a current EAP.
- 16.2. All locations must plan for fire, natural disasters (such as flood, tornado, and hurricane) and bomb threats.
- 16.3. For fire, natural disasters, and bomb threats, plan for keeping the material secure until order returns.
- 16.4. The person most familiar with the amount and significance of the COMSEC material on hand (normally the CRO) must prepare the plan.
- 16.5. If the plan calls for destroying COMSEC material, the CRO must make sure all destruction material and devices are readily available.
- 16.6. The plan must be realistic to accomplish its goals. Keep the plan simple.
- 16.7. Duties must be clear and concise.
- 16.8. Each person with access to COMSEC material must know of the plan and its location.
- 16.9. Conduct reviews and training exercises at least once a year.
- 16.10. Keep the plan current and revise it if necessary, based on the training exercises.

17. Communications Security Incident Reporting. The importance of reporting all known or suspected COMSEC incidents immediately cannot be overemphasized. Before issuing material or equipment, the COMSEC manager and the CRO must ensure users know they must immediately report known, suspected, or possible incidents of compromised COMSEC materials. Some specific actions you must report are:

17.1. **Physical Incidents.** Loss of control, theft, recovery by salvage, improper destruction, tampering, unauthorized viewing, access, copying, etc.

17.2. **Personnel Incidents.** Any capture, attempted recruitment, known or suspected control by a hostile intelligence entity, or unauthorized absence or defection of an individual who knows or has access to COMSEC material.

17.3. **Cryptographic Incidents.** Any equipment malfunction or operator error that threatens the security of a cryptographic machine, auto-manual, or manual cryptographic system, including unauthorized use of COMSEC keying material or equipment.

18. Education & Training.

18.1. In accordance with CMS 21A, Article 450, all COMSEC users must complete the COMSEC Material System Local Holder Custodian Training, computer based training (CBT) and all applicable sections of the CMS Personnel Qualification Standard. All completion certificates must be maintained by the Unit CRO and a copy forwarded to the FW Custodian.

18.2. Upon appointment as a Unit CRO all personnel will be required to complete CRO training. Coordination will be accomplished upon FW Custodian's receipt of the appointment letter. The training will be documented via AFCOMSEC Form 30.

18.3. Staff Assistance Visits will be conducted semi-annually for all units that receive COMSEC material via the FW COMSEC Custodian. A report of findings will be forwarded to the unit commander and a copy will be given to the Unit CRO for corrective action.

19. Cryptographic Access Program (CAP). IAW AFI 33-210, *Cryptographic Access Program*, the purpose of the CAP is to provide guidelines and procedures to grant access to classified cryptographic information the DoD produces, owns and controls. It is designed to prevent the loss or unauthorized disclosure of U.S. cryptographic information by ensuring access is granted only to individuals who satisfy the access and eligibility criteria. The FW COMSEC Custodians serve as the primary and alternate CAP Administrators. The CAP Administrators will determine based on criteria outlined in AFI 33-210 which unit individuals require CAP access. These individuals will be notified, receive a security briefing and complete all the necessary paperwork.

20. Forms Prescribed. AF Form 1109, **Visitor Register Log**, SF Form 153, **COMSEC Material Report**, and AFCOMSEC Form 30, **COMSEC Responsible Officer and User Training Checklist**.

BY ORDER OF THE GOVERNOR

BENNETT C. LANDRENEAU
Major General, LAARNG
The Adjutant General

OFFICIAL

//Signed//

JOHN B. SOILEAU, JR., COL, LA ANG
Acting ESSO

Attachments:

1. Glossary of References and Supporting Information
2. Appointment Letter for COMSEC
3. COMSEC Access List
4. CMS Responsibility Acknowledgement Form
5. Request for COMSEC Material Letter

Attachment 1

Glossary of References and Supporting Information

References

AFI 31-401, *Information Security Program Management*
AFPD 33-2, *Information Protection*
AFI 33-210, *Cryptographic Access Program*
AFI 33-211, *Communications Security (COMSEC) User Requirements*
AFI 33-212, *Reporting COMSEC Deviations*
DOD 5200.1-R, *Information Security Program*
CMS 21A, *Communications Security Material System Policy and Procedures for Navy Electronic Key Management System Tiers 2&3*
NASJRBNOINST 2280.1F, *Handling and Control of Communications Security Material System Distributed Material*

Abbreviations and Acronyms

AFI – Air Force Instruction
AFPD – Air Force Policy Directive
ALC – Accounting Legend Code
CAP – Cryptographic Access Program
CBT – Computer Based Training
CMS – Communications Security Material System
COMSEC – Communications Security
CRO – COMSEC Responsible Officer
EAP – Emergency Action Plan
EKMS – Electronic Key Management System
FW – Fighter Wing
GSA – General Services Administration
OI – Operating Instruction
STE - Secure Terminal Equipment
STU – Secure Telephone Unit

Attachment 2**SAMPLE APPOINTMENT LETTER FOR COMSEC RESPONSIBLE OFFICER AND
ALTERNATE**

LOUISIANA AIR NATIONAL GUARD
(Your Unit)

(Date)

MEMORANDUM FOR 159FW COMSEC CUSTODIAN

FROM: (Your Unit/Office Symbol)

SUBJECT: Designation of COMSEC Responsible Office (CRO)

1. The individuals listed below have been appointed the COMSEC Responsible Officers (CRO) for COMSEC material to be used by the **(your unit and office symbol)**. Appointee can receive and carry all COMSEC materials issued to this unit. They will ensure that the materials received are properly safeguarded in accordance with prescribed directives.

Name	Rank	SS#	Clearance
Primary			
Alternate			

2. All personnel listed hereon have been granted access to classified information and appropriate documentation is on file.

(Your Commander's Signature Block)
Commander

**THIS DOCUMENT CONTAINS PRIVACY ACT INFORMATION AND IS TO BE USED FOR THE
PURPOSE OF IDENTIFYING PERSONNEL APPOINTED AS CRO FOR THE UNIT REFERENCED.**

Attachment 3

SAMPLE COMSEC ACCESS LIST

LOUISIANA AIR NATIONAL GUARD
(Your Unit)

(Date)

MEMORANDUM FOR RECORD

FROM: (Your Unit/Office Symbol)

SUBJECT: Authorized Access to COMSEC Material

The following named personnel, this organization are authorized access to COMSEC material located in the **(building and room number)**.

Name	SSN	Clearance Level

(Your Commanders Signature Block)
Commander

THIS DOCUMENT CONTAINS PRIVACY ACT INFORMATION AND IS TO BE USED FOR THE PURPOSE OF IDENTIFYING PERSONNEL REQUIRING ACCESS TO COMSEC MATERIAL FOR THE UNIT REFERENCED ONLY.

Attachment 4**CMS RESPONSIBILITY ACKNOWLEDGEMENT FORM**

FROM: _____
(Rank, Full Name, SSN, and Unit)

TO: 159th Fighter Wing COMSEC Custodian

SUBJECT: CMS RESPONSIBILITY ACKNOWLEDGEMENT

Ref: (a) CMS 21A, Communications Security Material System Policy and Procedures for Navy Electronic Key Management System Tiers 2&3

(b) AFI33-211, Communications Security (COMSEC) User Requirements

1. I hereby acknowledge that I have read and understand the above references.
2. I assume full responsibility for the proper handling, storage, inventorying, accounting, and disposition of the COMSEC material held in my custody and/or used by me.
3. If at any time I am in doubt as to the proper handling of COMSEC material that I am responsible for, I will immediately contact my COMSEC Responsible Officer (CRO) and request advice.
4. I have read and understand the following excerpts.

AFI33-211, Communications Security (COMSEC) User Requirements (Excerpt)

4.4. COMSEC Users. COMSEC users have access to COMSEC aids and the responsibility for safeguarding them. COMSEC's ultimate success or failure rests with the material's individual users. The careless user or the user who fails to follow procedures for using, safeguarding, and destroying COMSEC material wastes all security efforts. COMSEC users must make sure that anyone who receives materials has authorization. Users must follow all security rules at all times and report to the CRO or COMSEC manager any circumstances or intentional or inadvertent acts that could lead to disclosure of classified information, including its loss, improper use, unauthorized viewing, or any other instance that could possibly jeopardize the value of COMSEC aides. COMSEC users:

- 4.4.1. Safeguard and control COMSEC material locally until they destroy it or turn it in.
- 4.4.2. Return material to CROs on request.
- 4.4.3. Familiarize themselves with correct procedures for operating associated cryptographic equipment and devices using applicable AFKAOs, KAOs, or instructions provided by the CRO.
- 4.4.4. Report immediately any known or suspected compromise of COMSEC material to the CRO or COMSEC manager.

CMS 21, CMS Policy and Procedure for Navy Tier 2 Electronic Key Management System (Excerpt)

Chapter 5 – SAFEGUARDING, STORAGE, ACCESS

501. GENERAL

a. Each person involved in the use of COMSEC material is personally responsible for:

- (1) Safeguarding and properly using the material they use or for which they are responsible.
- (2) Promptly reporting to proper authorities any occurrence, circumstance, or act which could jeopardize the security of COMSEC material.

Signature: _____

Date: _____

THIS DOCUMENT CONTAINS PRIVACY ACT INFORMATION AND SHOULD BE USED ONLY FOR THE PURPOSE OF IDENTIFYING USERS THAT ACKNOWLEDGE RESPONSIBILITY FOR THE PROPER HANDLING OF COMSEC MATERIAL.

Attachment 5

SAMPLE REQUEST FOR COMSEC MATERIAL LETTER

LOUISIANA AIR NATIONAL GUARD
(Your Unit)

(Date)

MEMORANDUM FOR 159FW COMSEC CUSTODIAN

FROM: (Your Unit/Office Symbol)

SUBJECT: Request For COMSEC Materials

1. Request a requirement be established for the following COMSEC material:

Short Title	Current Requirement	New Level

2. Justification:

3. Requested In-Place Date:

5. If further information is required please contact the undersigned at (your extension).

(CRO Signature Block)
CRO