

19 MAY 2000



Communications and Information

CRYPTOGRAPHIC ACCESS PROGRAM

COMPLIANCE WITH THIS PUBLICATION IS MANDATORY

NOTICE: This publication is available digitally on the AFDPO WWW site at: <http://afpubs.hq.af.mil>.

OPR: HQ AFCA/GCIS (Ms. Debbie Sellinger)

Certified by: HQ USAF/SCXX
(Lt Col Terry G. Pricer Sr.)

Supersedes AFI 33-210, 1 October 1998.

Pages: 16
Distribution: F

This Air Force instruction (AFI) implements Department of Defense Directive (DoDD) 5205.8, *Access to Classified Cryptographic Information*, February 20, 1991; National Telecommunications and Information Systems Security Policy (NTISSP) No. 3, *National Policy for Granting Access to U.S. Classified Cryptographic Information*, 19 December 1988; and Air Force Policy Directive (AFPD) 33-2, *Information Protection*. It establishes the Air Force Cryptographic Access Program (CAP) and provides guidelines and procedures to grant access to classified cryptographic information the DoD produces, owns, or controls. The purpose is to prevent loss or unauthorized disclosure of United States (U.S.) classified cryptographic information by ensuring access is granted to only individuals who satisfy the access and eligibility criteria identified within this instruction. Major commands (MAJCOM), field operating agencies, and direct reporting units may supplement this instruction only by coordinating with Headquarters Air Force Communications Agency (HQ AFCA/GCI), 203 W. Losey Street, Room 2040, Scott AFB IL 62225-5222. Send recommended changes or comments to HQ AFCA/ITPP, 203 West Losey Street, Room 1060, Scott AFB IL 62225-5222, through appropriate channels, using AF Form 847, **Recommendation for Change of Publication**, with an information copy to HQ AFCA/GCI and Headquarters Air Force Communications and Information Center (HQ AFCIC/SYNI), 1250 Air Force Pentagon, Washington DC 20330-1250. Refer conflicts between this AFI and other Air Force publications to HQ AFCA/ITPP, 203 W. Losey Street, Room 1060, Scott AFB IL 62225-5222. This instruction requires the collection and, or maintenance of information protected by the Privacy Act (PA) of 1974 authorized by Title 10 United States Code, Section 8013, Secretary of the Air Force, Powers and Duties. System of Records Notice F030 AF A, *Biographical Data and Automated Personnel Management System*, applies. Forms affected by the PA have an appropriate PA statement. See **Attachment 1** for the Glossary of References and Supporting Information.

SUMMARY OF REVISIONS

This interim change (IC) incorporates IC 2000-1 (**Attachment 4**) and specifies that a final security clearance is needed for cryptographic access eligibility. The IC defines HQ AFCA/GCI responsibilities for

Report Documentation Page

Report Date 19 May 2000	Report Type N/A	Dates Covered (from... to) -
Title and Subtitle Air Force Instruction 33-210, Communications and Information Cryptographic Access Program	Contract Number	
	Grant Number	
	Program Element Number	
Author(s)	Project Number	
	Task Number	
	Work Unit Number	
Performing Organization Name(s) and Address(es) Secretary of the Air Force Pentagon Washington, DC 20330-1250	Performing Organization Report Number AFI33-210	
Sponsoring/Monitoring Agency Name(s) and Address(es)	Sponsor/Monitor's Acronym(s)	
	Sponsor/Monitor's Report Number(s)	
Distribution/Availability Statement Approved for public release, distribution unlimited		
Supplementary Notes		
Abstract		
Subject Terms		
Report Classification unclassified	Classification of this page unclassified	
Classification of Abstract unclassified	Limitation of Abstract UU	
Number of Pages 16		

this program. It changes the date format making it compatible with an updated AFCOMSEC Form 9, **Cryptographic Access Certificate**. One paragraph was added concerning reporting requirements licensing. The IC also rewrites paragraph 7. to include the administrative withdrawal, suspension, and revocation process. Additionally, this IC corrects some minor administrative items. A (l) indicates revision from the previous edition.

1. General . Personnel occupying the following positions, that require continuing access to cryptographic information, must consent to the requirements of the CAP before getting access to cryptographic material:

- 1.1. Personnel assigned to communications security (COMSEC) accounts.
- 1.2. Personnel with access to TOP SECRET cryptographic media.
- 1.3. Personnel who operate key-generating equipment (for example, KG-83, KOK-22).
- 1.4. Personnel who operate certification authority workstations.
- 1.5. Personnel who assess/audit COMSEC management.
- 1.6. Personnel who prepare, authenticate, or decode nuclear control orders (valid or exercise).
- 1.7. Personnel assigned to secure communications facilities whose duties require keying of five or more different types of cryptographic equipment (that is, KG-84, KY-57, KY-65, KG-94, KG-194).
- 1.8. Personnel who perform duties as cryptographic maintenance, engineering, or installation technicians.
- 1.9. Personnel who receive, stock, store, package, and ship COMSEC material for COMSEC accounts 616600, 640000, and 670000. **NOTE:** When considering whether an individual should be enrolled in the CAP, do not use the fact that the individual simply has access to COMSEC material as the determining factor. Only submit AFCOMSEC Form 9 on individuals who meet the criteria in paragraphs 1.1. through 1.9. above.
- 1.10. The reporting requirements established in this AFI are exempt from licensing according to AFI 37-124, *The Information and Collections Reports Management Program Controlling Internal, Public, and Interagency Air Force Information Collections* (converting to AFI 33-324).

2. Responsibilities .

- 2.1. HQ AFCA/GCI. Manages the database for all AFCOMSEC Forms 9 and account update lists, and tracks polygraph testing. Provides the Office of Special Investigations with a yearly report for those needing polygraph testing. Notifies managers of anyone who has had status revoked or is in a suspended status.
- 2.2. COMSEC Managers. Oversee the CAP and provide written local procedures to all CAP administrators of personnel identified in paragraph 1.
- 2.3. Unit Commanders. Appoint, in writing, a CAP administrator to grant and withdraw cryptographic access and witness signatures on AFCOMSEC Forms 9.

2.4. The CAP Administrator. Identifies and grants cryptographic access in the commander's name to all personnel who require authorized access to classified cryptographic information. Provides a copy of the CAP administrator appointment letter to the COMSEC manager. If the COMSEC responsibility officer (CRO) is also performing duties as the CAP administrator, identifies both appointments in a single letter.

3. Cryptographic Access Eligibility . To qualify for cryptographic access, a person must meet all of the following qualifications:

3.1. Hold U.S. citizenship.

3.2. Be a DoD civilian employee, a DoD-cleared contractor or contractor employee, or a military service member.

3.3. Require cryptographic access to perform official duties.

3.4. Have a final security clearance and security investigation appropriate to the classified cryptographic information level accessed.

3.5. Receive a security briefing detailing the sensitive nature of cryptographic material and the individual's responsibility to protect cryptographic material (see [Attachment 2](#)).

3.6. Report contacts with individuals of any nationality to their security manager or supervisor when illegal or unauthorized access is sought to classified or sensitive information, or there is a concern that they may be the target of exploitation by a foreign entity (see AFI 31-501, *Personnel Security Program Management*).

3.7. Consent to periodic counterintelligence security non-lifestyle polygraph examinations and sign the AFCOMSEC Form 9 that contains both the cryptographic access certification and the polygraph consent.

4. Cryptographic Access .

4.1. For each individual covered in paragraph [1](#), the CAP administrator must follow these certification procedures:

4.1.1. Prepare an AFCOMSEC Form 9 in three copies. Submit the signed original to HQ AFCA/GCI, provide the second copy to the individual, and file the third copy. Type the form accurately and completely by using the AFCOMSEC Form 9. HQ AFCA/GCI returns all improperly completed AFCOMSEC Forms 9. Provide the following information:

4.1.1.1. Social Security Number (SSN).

4.1.1.2. Name (include "Jr.," "Sr.," or "III" after middle initial).

4.1.1.3. Date Granted Access. Year (YYYY), Month (MM), Day (DD) (use the date that the individual signs the AFCOMSEC Form 9).

4.1.1.4. Supporting COMSEC Account Number (DO NOT list user sub-account numbers).

4.1.1.5. Unit and Office Symbol.

4.1.1.6. Assigned Installation (enter the base or location of permanent assignment).

4.1.2. Brief personnel requiring cryptographic access at temporary duty (TDY) locations before they leave their home station. Include the individuals' access status on all clearance status notifications. Individuals will hand carry a copy of the AFCOMSEC Form 9 to their TDY location. This verifies the individuals' access status and provides a file copy for the TDY location. If the individuals' access status is not provided, check with the individuals' CAP administrator to verify if they are in the CAP at their permanent duty station. If individuals are not contained in the CAP, brief them at the TDY location and debrief them before they depart the TDY location. If the TDY is short notice, the COMSEC users will handle TOP SECRET materials, and if they are not previously briefed, brief the items below, as a minimum, using AFCOMSEC Form 30, **COMSEC Responsible Officer and User Training Checklist**, to document this briefing.

4.1.2.1. Issuing TOP SECRET material to COMSEC users; protective packaging and status information.

4.1.2.2. Transporting TOP SECRET material.

4.1.2.3. Two-person integrity (TPI) of TOP SECRET keying material.

4.1.2.4. Physical security requirements; access controls and procedures; storage of TOP SECRET COMSEC material; record of combinations; and daily security checks.

4.1.2.5. Use of TOP SECRET COMSEC material.

4.1.2.6. Inventory and accounting requirements, including the AFCOMSEC Form 16, **COMSEC Account Daily—Shift Inventory**.

4.1.2.7. Routine destruction: destruction and witnessing officials, destruction reports, and destruction methods.

4.1.2.8. Reporting TPI incidents.

4.1.2.9. TPI waivers.

4.1.2.10. Emergency destruction.

4.1.3. Submit name changes on a new AFCOMSEC Form 9, with the individual's SSN, to HQ AFCA/GCI, or make the change on the cryptographic access verification listing.

4.2. HQ AFCA/GCI maintains the original access certificate on file.

5. Polygraph Examinations . The Air Force Office of Special Investigations (AFOSI) regional polygraph offices, in conjunction with the HQ AFOSI Polygraph Division (HQ AFOSI/XOY), schedules and administers non-lifestyle polygraph examinations. HQ AFCA/GCI maintains a list of all persons who currently have cryptographic access status and periodically provides copies to AFOSI regional polygraph offices.

6. Cryptographic Access Program Verification Lists .

6.1. HQ AFCA/GCI semiannually sends a local list of the CAP database to each supporting COMSEC account.

6.2. COMSEC managers provide a copy of the CAP verification list to the CAP administrators to compare this list to those persons currently having access to ensure an accurate database. Instructions accompany each list.

6.3. Units and CAP administrators may request CAP verification lists from HQ AFCA/GCI through their supporting COMSEC manager.

7. Access Withdrawal . CAP administrators withdraw an individual's access by one of the following three methods:

7.1. Administrative Withdrawal. Applies to personnel reassigned to another base or unit to positions that do not require cryptographic access. The CAP administrator completes Section 3 of the AFCOMSEC Form 9 originally signed by the individual by placing an "X" in the "Administrative" box, placing date access withdrawn, and signing. Make two copies, submit the signed original to HQ AFCA/GCI, provide the second copy to the individual (when available), and maintain a copy in a transitory file.

7.2. Suspension. Applies to personnel who have their security clearance or other special access suspended in accordance with AFI 31-501. Suspend these individuals from duties requiring cryptographic access until the Air Force adjudicates the case. Review suspensions every 90 days and provide updates to HQ AFCA/GCI. Upon favorable adjudication, submit a new AFCOMSEC Form 9 changing the individual's status to active in the CAP database. Upon unfavorable adjudication, submit a new AFCOMSEC Form 9 that changes the individual's withdrawal status to administrative withdrawal or permanent revocation. Notify the COMSEC Manager.

7.2.1. The CAP administrator completes Section 3 of the copy of the AFCOMSEC Form 9 originally signed by the individual by placing an "X" in the "Suspension" box, annotating date access withdrawn, and signing. The unit commander or the civilian equivalent (for contractor accounts, the facility security manager) must sign the AFCOMSEC Form 9. Make two copies, submit the signed original to HQ AFCA/GCI, provide the second copy to the individual, and maintain a copy until adjudication is completed. The CAP administrator sends a letter with the AFCOMSEC Form 9 to HQ AFCA/GCI or a message stating the reason for suspension (see [Attachment 3](#)). Stamp correspondence containing reasons for the withdrawal FOR OFFICIAL USE ONLY.

7.2.2. If an individual is suspended from access with a security information file and then separates or is discharged from the Air Force before the investigation is completed, the commander determines the individual's trustworthiness by designating the withdrawal category on AFCOMSEC Form 9. Withdraw the person administratively if the individual is trustworthy. (**NOTE:** Follow the instructions in paragraph [7.1.](#))

7.3. Revocation. Applies to personnel who have their security clearance eligibility revoked, have their special access denied, or are permanently removed for cause. If the individual's cryptographic access is revoked it can never be reinstated, even if their security clearance eligibility is reinstated (see AFI 31-501). Notify the COMSEC manager. The CAP administrator completes Section 3 of the copy of the AFCOMSEC Form 9 originally signed by the individual by placing an "X" in the "Revocation" box, annotating date access withdrawn, and signing. The unit commander or the civilian equivalent (for contractor accounts, the facility security manager) must sign this AFCOMSEC Form 9. Make two copies, submit the signed original to HQ AFCA/GCI, provide a copy to the individual (if available), and maintain a copy in a transitory file. The CAP administrator sends a letter along with the AFCOMSEC Form 9 to HQ AFCA/GCI or a message stating the reason for the revocation (see [Attachment 3](#)). Stamp correspondence containing reasons for the withdrawal FOR OFFICIAL USE ONLY.

7.3.1. DELETED.

7.3.2. DELETED.

7.4. Notify the COMSEC manager for suspensions, revocation, or any individual declining cryptographic access.

7.4.1. DELETED.

7.4.2. DELETED.

7.4.3. DELETED.

7.4.4. DELETED.

7.4.5. DELETED.

8. Certificates of Personnel Declining Cryptographic Access . The CAP administrator sends HQ AFCA/GCI the original AFCOMSEC Form 9 for individuals who decline access. These certificates contain all the information on the individual except the signature. In the form's "Payroll Signature of Above Named Individual" block, enter: Individual Refused to Accept Cryptographic Access.

9. Commander's Administrative Actions on Personnel Declining Cryptographic Access or Polygraph Testing. As a condition of access to cryptographic information, an individual must sign the AFCOMSEC Form 9.

9.1. Commanders deny cryptographic access to personnel who decline to sign the AFCOMSEC Form 9 or who refuse to take a particular polygraph examination after previously giving their consent.

9.2. Persons denied access to cryptographic information for refusing to consent to polygraph examinations may not be assigned to positions requiring access to cryptographic information. If refusal occurs after assignment, a civilian employee is reassigned to a position of equal pay and grade in the Air Force, if available, or to such a position in another DoD component. If no such position is available, the civilian employee must be offered positions of lesser grade or pay, if available. Otherwise, employment in federal service is terminated. Air Force members ineligible for a cryptographic position for refusing to consent to a polygraph examination are reassigned as provided in military personnel regulations. No disciplinary action may be taken concerning employees or members who refuse to consent to polygraph examinations required as a condition for access to certain cryptographic information.

9.3. When a polygraph examination indicates deception, the examiner first attempts to resolve the issue in a post-examination interview. If that is unsuccessful, and the matter raises serious questions relevant to access, conduct another polygraph examination. If it does not resolve the issue, then conduct a comprehensive investigation.

9.3.1. Authorize adverse action only when this investigation discloses derogatory information that independently justifies the adverse action. However, only base adverse action solely on the polygraph examination if the Secretary of the Air Force personally determines that the cryptographic information is of such extreme sensitivity that access under the circumstances poses an unacceptable risk to the national security.

9.4. Administratively withdraw persons who refuse a polygraph examination after initially consenting.

10. Form Prescribed . AFCOMSEC Form 9, Cryptographic Access Certificate.

GARY A. AMBROSE, Brig Gen, USAF
Acting Director, Communications and Information

Attachment 1**GLOSSARY OF REFERENCES AND SUPPORTING INFORMATION*****References***

DoDD 5205.8, *Access to Classified Cryptographic Information*, February 20, 1991

DoDD 5210.48, *Access to Classified Cryptographic Information*

AFPD 33-2, *Information Protection*

AFI 31-501, *Personnel Security Program Management*

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

AFKAG-1, *Air Force Communications Security (COMSEC) Operations*

NTISSP No. 3, *National Policy for Granting Access to U.S. Classified Cryptographic Information*

Privacy Act of 1974

System of Records Notice F030 AF A, *Biographical Data and Automated Personnel Management System*

Title 10 U.S.C., Section 8013, *Secretary of the Air Force, Powers and Duties*

Uniform Code of Military Justice

Abbreviations and Acronyms

AF—Air Force (used on forms only)

AFCOMSEC—Air Force Communications Security

AFI—Air Force Instruction

AFOSI—Air Force Office of Special Investigations

CAP—Cryptographic Access Program

COMSEC—Communications Security

CRO—COMSEC Responsible Officer

DoD—Department of Defense

DoDD—Department of Defense Directive

HQ AFCA—Headquarters, Air Force Communications Agency

HQ AFCIC—Headquarters, Air Force Communications and Information Center

HQ USAF—Headquarters, United States Air Force

MAJCOM—Major Command

NTISSP—National Telecommunications and Information Systems Security Policy

PA—Privacy Act

SSN—Social Security Number

TDY—Temporary Duty

TPI—Two-person integrity

U.S.—United States

Terms

Access—The capability and opportunity to gain knowledge of or to alter information or material.

AFKAG—A short title used on general operational AF COMSEC publications. Publications are controlled in COMSEC channels.

Classified Cryptographic Information—1. Cryptographic keys and authenticators classified and designated as CRYPTO. 2. Classified cryptographic media that embody, describe, or implement a classified cryptographic logic, including depot-level maintenance manuals, cryptographic descriptions, drawings of cryptographic logic, specifications describing a cryptographic logic, and cryptographic computer software.

Cryptographic Access Program (CAP)—A program to protect national security information and govern access to cryptographic information that the DoD produces, controls, or owns.

CAP Administrators—Individuals responsible for granting and withdrawing cryptographic access within a particular unit. Commanders appoint CAP administrators.

Attachment 2**CRYPTOGRAPHIC ACCESS BRIEFING**

A2.1. You were selected to perform duties that will require access to U.S. classified cryptographic information. Before the Air Force grants you this access, you must understand the safeguards that protect this information, the directives that govern authorized access, and the penalties you will incur for the unauthorized disclosure, unauthorized retention, or negligent handling of U.S. classified cryptographic information. Failure to properly safeguard this information could cause serious to exceptionally grave damage or irreparable injury to the national security of the United States.

A2.2. U.S. classified cryptographic information is especially sensitive because we use it to protect classified information. You can use any particular piece of cryptographic keying material and any specific cryptographic technique to protect a large quantity of classified information during transmission. If the integrity of a cryptographic system is breached at any point, all information protected by the system might be compromised. The safeguards placed on U.S. classified cryptographic information is a necessary component of government programs to make sure material vital to our national security remains SECRET.

A2.3. Because access to U.S. classified cryptographic information is granted on a strict need-to-know basis, you will only receive access to the cryptographic information necessary to perform your duties. You must become familiar with AFI 33-211, Communications Security (COMSEC) User Requirements, or AFKAG-1, *Air Force Communications Security (COMSEC) Operations*, as appropriate.

A2.4. Timely reporting of any known or suspected compromise of U.S. classified cryptographic information is especially important. If a compromised cryptographic system goes unreported, our continued use of the system can result in the loss of all the information it protects. If you report the compromise, we can take steps to lessen an adversary's advantage gained through the compromise of the information.

A2.5. As a condition of having access to U.S. cryptographic information, you must sign AFCOMSEC Form 9. When you sign this form you are acknowledging that you are subject to, and consenting to, periodic counterintelligence-scope polygraph examinations. This examination is administered according to the provisions of DoDD 5210.48, *Access to Classified Cryptographic Information*, and applicable law. This polygraph examination only encompasses questions concerning disloyal activities, espionage, sabotage, terrorism, and general honesty and trustworthiness.

A2.6. You have the right to refuse to take a counterintelligence-scope polygraph examination. If you refuse to take the examination, we will deny you access to U.S. classified cryptographic information. A denial of access to classified cryptographic information may result in reassignment to another position at the same grade and pay, if one is available. If a similar position is not available, you may be offered a position at a lesser grade and pay. Your refusal will not be recorded in your personnel or investigative file. However, if you do not want to sign the cryptographic access at this time, I will terminate this briefing and the briefing administrator will record your decision on the cryptographic access certificate. Choosing not to sign the certificate has the same effect as refusing to take the examination.

A2.7. The intelligence services of some foreign governments prize the acquisition of U.S. classified cryptographic information. They will go to extreme lengths to compromise U.S. citizens and force them

to divulge cryptographic techniques and materials that protect the nation's secrets around the world. You must understand that any personal or financial relationship with a foreign government's representative could make you vulnerable to attempts at coercion. You must stay alert so that you can recognize and counter such attempts. The best personal policy is to avoid discussions that reveal your knowledge of, or access to, U.S. classified cryptographic information. You must report any attempt, either through friendship or coercion, to solicit your knowledge regarding the U.S. classified cryptographic information you possess immediately to your commander or local AFOSI office. You must also report any unofficial foreign travel to your local security manager so you may receive specific information concerning security issues related to your foreign travel.

A2.8. In view of these risks, you must agree to report contacts with individuals of any nationality to your security manager or supervisor when illegal or unauthorized access is sought to classified or sensitive information, or there is a concern that you may be the target of exploitation by a foreign entity.

A2.9. Finally, you must be aware that if you willfully or negligently disclose U.S. classified cryptographic information to any unauthorized persons, you are subject to administrative and civil sanctions, including adverse personnel actions, as well as criminal sanctions under the Uniform Code of Military Justice and the criminal laws of the United States.

Attachment 3**SAMPLE MESSAGES****A3.1. Reason for Suspension .**

DATE TIME GROUP

FM 123BW ANYWHERE AFB TX//DOC//

TO HQ AFCA SCOTT AFB IL//GCIC//

INFO 123SQ ANYWHERE AFB TX//CA654321//

UNCLAS FOUO

SUBJ: CHANGE IN CRYPTOGRAPHIC ACCESS STATUS

1. THE CRYPTOGRAPHIC ACCESS FOR JOHN Q. DOE, SSN 123-45-6789, WAS SUSPENDED DUE TO (STATE REASON FOR SUSPENSION).
2. AFCOMSEC FORM 9 MAILED 22 OCT 97.
3. POC IS MSGT MANAGER OR SGT ACCOUNTANT, DSN 555-1234.

A3.2. Ninety (90)-Day Update for Suspension .

DATE TIME GROUP

FM 123BW ANYWHERE AFB TX//DOC//

TO HQ AFCA SCOTT AFB IL//GCIC//

INFO 123SQ ANYWHERE AFB TX//CA654321//

UNCLAS FOUO

SUBJ: CHANGE IN CRYPTOGRAPHIC ACCESS STATUS

1. THIS IS THE FIRST 90 DAY STATUS UPDATE ON THE SUSPENSION OF JOHN Q. DOE, SSN 123-45-6789. INDIVIDUAL IS (STATE PENDING ACTION OR NO CHANGE IN STATUS).
2. POC IS MSGT MANAGER OR SGT ACCOUNTANT, DSN 555-1234.

A3.3. Reason for Revocation .

DATE TIME GROUP

FM 123BW ANYWHERE AFB TX//DOC//

TO HQ AFCA SCOTT AFB IL//GCIC//

INFO 123SQ ANYWHERE AFB TX//CA654321//

UNCLAS FOUO

SUBJ: CHANGE IN CRYPTOGRAPHIC ACCESS STATUS

1. THE CRYPTOGRAPHIC ACCESS FOR JOHN Q. DOE, SSN 123-45-6789, WAS REVOKED DUE TO (STATE REASON FOR REVOCATION).

2. AFCOMSEC FORM 9, SIGNED BY THE COMMANDER, MAILED 15 DEC 97.
3. POC IS MAJ COMMANDER, DSN 555-1234.

Attachment 4**IC 2000-1 TO AFI 33-210, CRYPTOGRAPHIC ACCESS PROGRAM**

19 MAY 2000

SUMMARY OF REVISIONS

This interim change (IC) incorporates IC 2000-1 (**Attachment 4**) and specifies that a final security clearance is needed for cryptographic access eligibility. The IC defines HQ AFCA/GCI responsibilities for this program. It changes the date format making it compatible with an updated AFCOMSEC Form 9, **Cryptographic Access Certificate**. One paragraph was added concerning reporting requirements licensing. The IC also rewrites paragraph 7. to include the administrative withdrawal, suspension, and revocation process. Additionally, this IC corrects some minor administrative items. A (l) indicates revision from the previous edition.

1.10. The reporting requirements established in this AFI are exempt from licensing according to AFI 37-124, *The Information and Collections Reports Management Program Controlling Internal, Public, and Interagency Air Force Information Collections* (converting to AFI 33-324).

2.1. HQ AFCA/GCI. Manages the database for all AFCOMSEC Forms 9 and account update lists, and tracks polygraph testing. Provides the Office of Special Investigations with a yearly report for those needing polygraph testing. Notifies managers of anyone who has had status revoked or is in a suspended status.

2.2. COMSEC Managers. Oversee the CAP and provide written local procedures to all CAP administrators of personnel identified in paragraph 1.

2.3. Unit Commanders. Appoint, in writing, a CAP administrator to grant and withdraw cryptographic access and witness signatures on AFCOMSEC Forms 9.

2.4. The CAP Administrator. Identifies and grants cryptographic access in the commander's name to all personnel who require authorized access to classified cryptographic information. Provides a copy of the CAP administrator appointment letter to the COMSEC manager. If the COMSEC responsibility officer (CRO) is also performing duties as the CAP administrator, identifies both appointments in a single letter.

3.4. Have a final security clearance and security investigation appropriate to the classified cryptographic information level accessed.

4.1.1. Prepare an AFCOMSEC Form 9 in three copies. Submit the signed original to HQ AFCA/GCI, provide the second copy to the individual, and file the third copy. Type the form accurately and completely by using the AFCOMSEC Form 9. HQ AFCA/GCI returns all improperly completed AFCOMSEC Forms 9. Provide the following information:

4.1.1.3. Date Granted Access. Year (YYYY), Month (MM), Day (DD) (use the date that the individual signs the AFCOMSEC Form 9).

7.1. Administrative Withdrawal. Applies to personnel reassigned to another base or unit to positions that do not require cryptographic access. The CAP administrator completes Section 3 of the AFCOMSEC Form 9 originally signed by the individual by placing an "X" in the "Administrative" box, placing date access withdrawn, and signing. Make two copies, submit the signed original to HQ AFCA/GCI, provide the second copy to the individual (when available), and maintain a copy in a transitory file.

7.2. Suspension. Applies to personnel who have their security clearance or other special access suspended in accordance with AFI 31-501. Suspend these individuals from duties requiring cryptographic access until the Air Force adjudicates the case. Review suspensions every 90 days and provide updates to HQ AFCA/GCI. Upon favorable adjudication, submit a new AFCOMSEC Form 9 changing the individual's status to active in the CAP database. Upon unfavorable adjudication, submit a new AFCOMSEC Form 9 that changes the individual's withdrawal status to administrative withdrawal or permanent revocation. Notify the COMSEC Manager.

7.2.1. The CAP administrator completes Section 3 of the copy of the AFCOMSEC Form 9 originally signed by the individual by placing an "X" in the "Suspension" box, annotating date access withdrawn, and signing. The unit commander or the civilian equivalent (for contractor accounts, the facility security manager) must sign the AFCOMSEC Form 9. Make two copies, submit the signed original to HQ AFCA/GCI, provide the second copy to the individual, and maintain a copy until adjudication is completed. The CAP administrator sends a letter with the AFCOMSEC Form 9 to HQ AFCA/GCI or a message stating the reason for suspension (see [Attachment 3](#)). Stamp correspondence containing reasons for the withdrawal FOR OFFICIAL USE ONLY.

7.2.2. If an individual is suspended from access with a security information file and then separates or is discharged from the Air Force before the investigation is completed, the commander determines the individual's trustworthiness by designating the withdrawal category on AFCOMSEC Form 9. Withdraw the person administratively if the individual is trustworthy. (**NOTE:** Follow the instructions in paragraph 7.1.)

7.3. Revocation. Applies to personnel who have their security clearance eligibility revoked, have their special access denied, or are permanently removed for cause. If the individual's cryptographic access is revoked it can never be reinstated, even if their security clearance eligibility is reinstated (see AFI 31-501). Notify the COMSEC manager. The CAP administrator completes Section 3 of the copy of the

AFCOMSEC Form 9 originally signed by the individual by placing an "X" in the "Revocation" box, annotating date access withdrawn, and signing. The unit commander or the civilian equivalent (for contractor accounts, the facility security manager) must sign this AFCOMSEC Form 9. Make two copies, submit the signed original to HQ AFCA/GCI, provide a copy to the individual (if available), and maintain a copy in a transitory file. The CAP administrator sends a letter along with the AFCOMSEC Form 9 to HQ AFCA/GCI or a message stating the reason for the revocation (see [Attachment 3](#)). Stamp correspondence containing reasons for the withdrawal FOR OFFICIAL USE ONLY.

7.3.1. DELETED.

7.3.2. DELETED.

7.4. Notify the COMSEC manager for suspensions, revocation, or any individual declining cryptographic access.

7.4.1. DELETED.

7.4.2. DELETED.

7.4.3. DELETED.

7.4.4. DELETED.

7.4.5. DELETED.

9. Commander's Administrative Actions on Personnel Declining Cryptographic Access or Polygraph Testing. As a condition of access to cryptographic information, an individual must sign the AFCOMSEC Form 9.

GARY A. AMBROSE, Brig Gen, USAF

Acting Director, Communications and Information