

**BY ORDER OF THE
SECRETARY OF THE AIR FORCE**

AIR FORCE SYSTEMS SECURITY INSTRUCTION 4100, VOLUME 1

1 August 1998

Communications and Information



★ THE AIR FORCE COMMUNICATIONS SECURITY (COMSEC) PROGRAM

COMPLIANCE WITH THIS PUBLICATION IS MANDATORY

NOTICE: This publication is available digitally on the Air Force Information Protection (to become Information Assurance) Home Page located at: <http://www.afca.scott.af.mil/ip>.

OPR: HQ AFCA/GCI (CMSgt Hogan)
Supersedes: AFSSI 4100, 15 December 1992

Certified by: HQ AFCA/GCI (Ronald G. Goessman)
Pages: 21
Distribution: F

This Air Force Systems Security Instruction (AFSSI) implements National Security Directive (NSD) 42, *National Policy for the Security of National Security Telecommunications and Information Systems*, DoD Directive C-5200.5(C), *Communications Security (COMSEC) (U)*, and Air Force Policy Directive (AFPD) 33-2, *Information Protection* (to become *Information Assurance*), and incorporates communications security policy from National Communications Security Committee (NCSC) 1, *National Policy for Safeguarding and Control of Communications Security Material*, NCSC-2, *National Policy on Release of Communications Security Information To U.S. Contractors and Other U.S. Nongovernmental Sources*, National Telecommunications and Information Systems Security Policy (NTISSP) No. 1, *National Policy on Application of Communications Security to U.S. Civil and Commercial Space Systems*, NSTISSP No. 8, *National Policy Governing the Release of Information Systems Security (INFOSEC) Products or Associated INFOSEC Information to Foreign Governments*, and DoD Instruction S-5225.1(S), *Communications Security (COMSEC) Assistance to Foreign Governments and International Organizations (U)*. This instruction applies to all Air Force military and civilian personnel, including Air National Guard and United States Air Force Reserve units and members, and to contractors performing operations in support of an Air Force contract. Unless otherwise specified, the term "major command" (MAJCOM), as used in this instruction, includes field operating agencies (FOA) and direct reporting units (DRU). The instruction prescribes procedures for securing and protecting information systems, COMSEC equipment, and material. It affects development, procurement, installation, and operation of all equipment used to process classified or sensitive information within the Air Force. Refer changes and conflicts between this and other publications through major command (MAJCOM) Information Assurance (IA) offices to Headquarters, Air Force Communications Agency, Global Connectivity Information Protection (to become Information Assurance) Division (HQ AFCA/GCI), 203 W. Losey Street Room 2040, Scott AFB, IL 62225-5234, using AF Form 847, **Recommendation for Change of Publication**, with an information copy to Air Force Communication and Information Center, Information Protection (to become Information Assurance) Branch (AFCIC/SYNI), 1250 Air Force Pentagon, Washington, DC 20330-1250. Refer technical questions on the content of this instruction to HQ AFCA/GCIS, 203 W. Losey Street, Room 2040, Scott AFB IL 62225-5234.

SUMMARY OF REVISIONS

FOR OFFICIAL USE ONLY

This document is substantially revised and must be completely reviewed. This instruction updates the responsibilities of the various agencies involved in communications security (COMSEC) and outlines and revises Air Force implementation instructions and procedures to more closely align with national and DoD COMSEC policy. This publication clarifies the requirements for securing or protecting (see definitions at attachment 1) U.S. Air Force information systems and provides a chart identifying the authorized methods of providing encryption for the various types of information. This document also revises procedures for requesting waivers to Air Force COMSEC requirements and release of U.S. government COMSEC products or information to foreign governments or international organizations.

1. Communications Security (COMSEC) Introduction. Continuing advances in microelectronics technology have stimulated an unprecedented growth in the demand for and supply of information systems services within the government and throughout the private sector. As new technologies have been applied, traditional distinctions between telecommunications and information systems have begun to disappear. Although this trend promises greatly improved efficiency and effectiveness, it also poses significant security challenges.

1.1. Threat to Information Systems. Information systems are highly susceptible to interception, unauthorized electronic access, and related forms of technical exploitation, as well as other dimensions of the foreign intelligence threat. The technology to exploit these electronic systems is widespread and is used extensively by foreign nationals and can be employed, as well, by terrorist groups and criminal elements. A comprehensive and coordinated approach must be taken to protect the government's national security information systems against current and projected threats.

1.2. COMSEC Protection. COMSEC refers to measures and controls taken to deny unauthorized persons information derived from information systems of the United States Government related to national security and to ensure the authenticity of such information systems. Communications security protection results from the application of security measures including cryptosecurity, transmission security, and emission security to information systems generating, handling, storing, processing, or using classified or sensitive government or government-derived information, the loss of which could adversely affect the national security interest. It also includes the application of physical security measures to COMSEC information or materials.

1.3. The Air Force COMSEC Program. Ensuring the security of national security systems is vitally important to the operational effectiveness of the national security activities of the government and to military combat readiness. The Air Force COMSEC program is established to meet the Public Law and national and DoD requirements to secure or protect classified, or sensitive information processed on Air Force information systems.

1.4. Terms Explained. See Attachment 1.

1.5. Classification Guidance. AFMAN 33-272 (S), *Classifying Communications Security, TEMPEST, and C4 Systems Security Research and Development Information (U)* (to become *Information Assurance Classification Guide*), provides classification guidance for COMSEC information. Direct requests for guidance or clarification to the appropriate MAJCOM Information Assurance (IA) office.

1.6. How to Request COMSEC Services, Support, Clarification, and Assistance. Air Force activities must submit requests for COMSEC services, support, clarification and assistance to their MAJCOM IA office. If further assistance is required, the MAJCOM IA office must request it from HQ AFCA/GCI. Only HQ AFCA or AFCIC/SYNI may request assistance from the National Security Agency (NSA) and then only when the capability is not available from Air Force resources. HQ AFMC may contact NSA directly on COMSEC research, development, testing, and evaluation matters according to AFI 63-102, *Communications-Computer Systems Security Research, Development, Test and Evaluation*.

2. COMSEC Responsibilities.

2.1. National Security Agency (NSA). The Director, NSA, is designated the National Manager for National Security Telecommunications and Information Systems Security and is responsible to the Secretary of Defense who is the Executive Agent of the Government for National Security Telecommunications and Information Systems Security. As such, the Director, NSA, is the DoD COMSEC Program Manager who acts as the DoD focal point for cryptography and communications security. In fulfilling these responsibilities, NSA:

2.1.1. Ensures the development of plans and programs to fulfill COMSEC objectives and develops plans, policies, procedures, and mechanisms to ensure that technology and products are available for DoD components and their contractors to satisfy their COMSEC requirements.

2.1.2. Conducts, approves, and endorses research and development of COMSEC techniques and equipment needed to fulfill cryptographic requirements of information systems.

2.1.3. Establishes standards and procedures and administers business techniques for the development and production of COMSEC products, systems, and services; conducts evaluations of and endorses them for use by DoD components; and determines the method of procurement.

2.1.3.1. NSA acts as the central procurement authority for COMSEC equipment, aids, and design-controlled spare parts when the method of procurement is direct by DoD components.

2.1.3.2. When NSA is not the central procurement authority, NSA authorizes commercial vendors to make direct sales and publishes and updates a compilation of all NSA-endorsed COMSEC products and their authorized sources.

2.1.4. Reviews and approves all COMSEC standards, techniques, equipment, and protected services and prescribes or approves all cryptographic systems and techniques used by or on behalf of the DoD to encrypt national security information (classified) and secure national security systems from foreign intelligence exploitation and disruption or to ensure authenticity.

2.1.5. Prescribes minimum standards, methods, and procedures for the management of key, including generation, production, storage, distribution, destruction, accounting, use protection, and compromise recovery.

2.1.5.1. Operates printing and fabrication facilities related to the provision of cryptographic and other technical security material or services.

2.1.5.2. Generates and produces COMSEC aids, including all forms of key and authorizes designated DoD activities to produce specified COMSEC equipment, aids, key, and cryptomaterial according to prescribed security criteria.

2.1.5.3. Maintains the consolidated office of record for all COMSEC material, and prescribes minimum security standards for the performance of COMSEC Central Office of Records (CORs) by DoD components.

2.1.5.4. Establishes procedures for reporting COMSEC incidents to include evaluation as to the probability of compromise, implementation of corrective actions, and initiation of COMSEC incident trend analysis reports.

2.1.6. Prescribes the minimum standards, methods, and procedures for protecting cryptographic and other technical security material, techniques, and information, and promulgates classification guidelines for COMSEC information.

2.1.7. Promotes efficient use of COMSEC equipment by formulating and disseminating procedures for the integrated management of DoD COMSEC equipment, establishing procedures for an inter-Department loan program, and maintaining a facility for the disposal of unserviceable or obsolete and the redistribution or disposal of excess COMSEC equipment.

2.1.8. Conducts and coordinates COMSEC assessment programs to continually examine the information systems of the Department of Defense and its contractors to include monitoring, assessing of system vulnerabilities and the adversary threat to these information systems, and disseminating assessment findings to DoD components and their contractors recommending appropriate countermeasures, and when requested, assist in the preparation of periodic evaluation of their security posture.

2.2. SAF/AQ. The Office of the Secretary of the Air Force (Acquisition) is responsible for providing direction to Air Force COMSEC research, development, test, and evaluation efforts.

2.3. SAF/IA. SAF/IA processes all approval transfers of COMSEC and related services for foreign governments and international organizations.

2.4. HQ USAF/IL. HQ USAF/IL develops concepts and establishes policy for integrated support and configuration management of COMSEC equipment and issues procurement authorizations for COMSEC resources that assure Air Force logistics support in peace and war.

2.5. HQ USAF/SC. HQ USAF/SC approves waivers for the use of other than NSA endorsed and NIST validated products, on Air Force systems, to protect sensitive information during transmission. This includes allowing use of products on a migration path to NIST validation.

2.6. Air Force Communications and Information Center (AFCIC)/SYNI. AFCIC/SYNI is responsible for:

2.6.1. Developing COMSEC doctrine, policy, procedures, and practices for the Air Force.

2.6.2. Functional planning, advocacy, and management of Air Force COMSEC resources, and designates, or delegates the designation of, Air Force controlling authorities according to AFI 33-215, *Controlling Authorities for COMSEC Keying Material (Keymat)*.

2.6.3. Planning and advocating Air Force COMSEC resources (funds and manpower).

2.7. Headquarters, Air Force Communications Agency (HQ AFCA). HQ AFCA will:

2.7.1. Provide AF COMSEC guidance and support to MAJCOMs, FOAs, DRUs, and wing IA offices.

2.7.2. Ensure Air Force contracting guidance reflects national, DoD, and Air Force COMSEC policy and procedures, in conjunction with AFCIC/SYNI.

2.7.3. Act as Lead Command for the Air Force Electronic Key Management System (AFEKMS).

2.7.4. During the technical review of waiver requests for the use of other than NSA endorsed and NIST validated products to protect sensitive information during transmission, determine if the request has Air

Force wide applicability, and if so, submit for inclusion in the Joint Technical Architecture - Air Force (JTA-AF).

2.8. Headquarters, Cryptologic Systems Group (HQ CPSG). HQ CPSG performs COMSEC material life cycle management which includes acquisition, item management, technical service, stock, storage, distribution, and final disposition; acts as the Air Force COR for accountable COMSEC material; and serves as the Program Management Office (PMO) for the AFEKMS.

2.9. Headquarters, Air Force Material Command (HQ AFMC):

2.9.1. Performs configuration management functions for systems using COMSEC equipment supported by AFMC.

2.9.2. Conducts the Air Force Communications-Computer Systems Security Research, Development, Test & Evaluation (RDT&E) Program according to AFI 63-102, *Communications-Computer Systems Security Research, Development, Test and Evaluation*.

2.9.3. Ensures advanced development programs are reviewed for compatibility with COMSEC equipment and systems.

2.10. Headquarters, Air Education & Training Command (HQ AETC). Trains personnel in proper COMSEC management, design, procurement, engineering, operation, maintenance, installation, and test and evaluation techniques to ensure uniform COMSEC practices throughout the Air Force.

2.11. MAJCOMs. MAJCOMs plan, organize, implement, and control MAJCOM COMSEC activities. MAJCOM COMSEC OPRs:

2.11.1. Ensure all levels of command consider COMSEC requirements in planning, designing, developing, testing and evaluating, training, installing, operating, and disposing of information systems and weapon and support systems or programs.

2.11.1.1. Coordinate command actions in support of approved National, DoD, and Air Force level COMSEC programs.

2.11.1.2. Regularly review plans and planning documents to ensure COMSEC requirements for operations, contingencies, and exercises are addressed and identified as required by AFMAN 10-401, *Operation Plan and Concert Plan Development and Implementation*.

2.11.1.2.1. Coordinate command input regarding COMSEC requirements with the plan's OPR and provide guidance on subordinate unit plans, when necessary.

2.11.1.2.2. Ensure plans identifying COMSEC requirements provide specific information to permit compliance with the basic instructions in this document.

2.11.1.3. Approve or disapprove telemetry waiver requests from field units according to paragraph 5.2. and forward a copy of all approved requests to HQ AFCA.

2.11.2. Provide COMSEC guidance, assistance, and command procedures to command staff and COMSEC accounts.

2.11.2.1. Maintain membership on command boards, panels, or working groups to provide COMSEC guidance to those activities and information relating to national security.

2.11.2.2. Establish and manage a command IP (to become IA) assessment and assistance program, according to AFI 33-230, *Information Protection Assessment and Assistance Program*, to assess and assist command implementation of COMSEC procedures.

2.11.2.2.1. The contracting command and/or COMSEC monitoring headquarters is responsible for quality assurance evaluation as it applies to handling and using COMSEC material.

2.11.2.2.2. The contracting command has full authority to conduct COMSEC audits of COMSEC accounts, or to assess and assist contractor implementation of COMSEC procedures.

2.11.2.3. Establish and maintain a reference library of COMSEC documents and information.

2.11.2.4. Include COMSEC in education and training programs. Review and use HQ AFCA's "COMSEC Incident/Insecurity Trends" messages to educate command COMSEC accounts and users about COMSEC trends.

2.11.2.5. Periodically evaluate and correct operational procedures or practices that weaken communications security.

2.11.3. Manage their command's portion of the DoD 5220.22M, *National Industrial Security Program Operating Manual*, according to AFI 31-601, *Industrial Security Program Management*, as it pertains to Air Force COMSEC matters.

2.12. Wing IA Office. AFKAG-1, *Air Force Communications Security (COMSEC) Operations*, outlines the specific COMSEC responsibilities of the office.

3. Planning for Communications and Information Systems. COMSEC requirements are an integral part of program planning for all information systems, including those integral to weapons systems and weapon support systems, and must be addressed throughout the system life cycle (e.g., concept definition, design and development, test and evaluation [T&E], procurement, installation, operation, maintenance, and disposal).

4. Cryptosecurity. Cryptosecurity is the component of COMSEC resulting from the provision of technically sound cryptosystems and their proper use.

4.1. Use of Approved COMSEC. As the DoD focal point for cryptography and communications security, NSA must approve or endorse all COMSEC standards, techniques, equipment, and protected services and prescribe or approve all cryptographic systems and techniques used by or on behalf of Department of Defense activities to encrypt classified and sensitive information, that is not subject to Public Law 100-235, from foreign intelligence exploitation and disruption or to ensure authenticity.

4.2. Acquiring COMSEC Material. DoD activities must acquire COMSEC products and services through NSA as the centralized COMSEC acquisition authority.

4.2.1. Headquarters, Cryptologic Systems Group (HQ CPSG), is the activity within the Air Force that acts on behalf of NSA as a centralized procurement authority.

4.2.1.1. After establishing a requirement for COMSEC equipment, the requiring activity (user) procures the equipment using standard supply procedures.

4.2.1.2. Consult your servicing COMSEC account for local procedures to establish a requirement for and obtain COMSEC aids.

4.2.2. If unavailable through centralized procurement, acquire COMSEC products and services directly from commercial entities authorized by NSA to sell such products and services.

5. Transmission Security (TRANSEC). TRANSEC is the component of COMSEC resulting from the application of measures designed to protect transmissions from interception and exploitation by means other than cryptanalysis.

5.1. TRANSEC Requirements. Information transmitted by information systems is highly susceptible to interception, technical exploitation, the human intelligence (HUMINT) threat, and other dimensions of the foreign intelligence threat. Security is a vital element of the effectiveness of national security activities and defense preparedness. Ensuring the security and protection of information systems that transmit classified and sensitive information is a national responsibility. Table 5-1, Applying Communications Security (COMSEC) to Assure Information, provides information identifying the minimum authorized method(s) of securing or protecting classified; sensitive; or a combination of classified and sensitive information during transmission.

5.2. TRANSEC Requirements for the Application of COMSEC to U.S. Civil and Commercial Space Systems. Protect both the relayed telecommunications transmitted over space system circuits and the command and control uplink. Limit government and government contractor use of civil space systems for information systems to those protected by approved techniques. The following Air Force COMSEC procedures implement national policy applicable to U.S. civil and commercial space systems:

5.2.1. Use NSA-approved COMSEC techniques to protect all government and government contractor classified and sensitive information transmitted over satellite circuits from exploitation by unauthorized interception.

5.2.2. Limit government or government-contractor use of U.S. civil (government-owned but non-DoD) and commercial satellites launched after 17 June 1990 to space systems using accepted techniques necessary to protect the command and control uplink.

5.2.3. Determine the need for and means to protect the command and control uplink associated with civil satellite systems, that are intended exclusively for unclassified missions, in coordination with NSA.

5.2.4. Submit waivers to these requirements according to Attachment 2.

5.3. Protected Distribution Systems (PDSs). A protected distribution system (PDS) is a wire line or fiber optic distribution system used to transmit unencrypted classified national security information through an area of lesser classification or control. AFSSI 3030, *Protected Distribution Systems*, implements national policy and contains guidance on the approval, construction requirements, and use of protected distribution systems within the Air Force.

6. Emission Security (EMSEC). Emission security is the protection resulting from measures taken to deny unauthorized persons information derived from intercept and analysis of compromising emanations from crypto-equipment or an Information System. AFI 33-203, *The Air Force Emission Security Program*, implements national and DoD EMSEC policy and contains instructions for applying EMSEC within the Air Force.

TABLE 5-1 APPLYING COMMUNICATIONS SECURITY (COMSEC) TO ASSURE INFORMATION

R U L E	A	B
	When transmitting information that is	secure or protect it using a
1	Classified	NSA endorsed Type 1 product (Notes 1 and 4)
2	A combination of classified and sensitive information	NSA endorsed Type 1 product (Notes 1 and 4)
3	Sensitive information which: involves intelligence activities, involves cryptologic activities related to national security, involves command and control of military forces, involves equipment that is an integral part of a weapon or weapon system, or is critical to the direct fulfillment of military or intelligence missions. NOTE: This type of information is formerly known as “Warner Amendment” type information	NSA endorsed Type 1 or 2 product (Notes 1, 4, 5, and 6), or a NIST validated product that meets security level 2 or higher (Note 2), or a HQ USAF/SC approved solution to a system level implementation that has been reviewed by NSA. (Note 8)
4	Any other type of business or administrative sensitive information such as financial, logistics, proprietary, source selection, personnel management, etc.	NSA endorsed Type 1 or 2 product (Notes 1, 4, 5, and 6), or a NIST validated product (Note 2), or a NSA evaluated product (Note 3), or a HQ USAF/SC approved product (Notes 7 and 8)

NOTES:

1. A listing of NSA endorsed Type 1 and Type 2 products can be found in the Information Systems Security Products and Services Catalogue and the Information System Security Manual.
2. NIST maintains a number of cryptographic standards and coordinates validation programs for many of those standards. The Cryptographic Module Validation (CMV) Program encompasses validation testing for cryptographic modules (FIPS 140-1), the Data Encryption Standard and its modes of operation (FIPS 46-2 and 81), the Secure Hash Standard (FIPS 180-1), and the Digital Signature Standard (FIPS 186). In accordance with FIPS 140-1, NIST validated products using a Type 3 algorithm receive a security level rating (1-4, from lowest to highest), depending on what requirements are met. A listing of NIST validated products, including the FIPS 140-1 Cryptographic Modules Validation List, can be found at <http://csrc.nist.gov/cryptval/>.
3. NSA evaluated products are commercial, off-the-shelf (COTS) products that NSA has evaluated, but not endorsed, against established commercial standards, to assess the effectiveness of the vendor’s advertised security controls.

4. A Type 1 product is a classified or controlled cryptographic item, endorsed by NSA, for securing classified and sensitive information, when appropriately keyed. The term refers only to products and not to information, key, services, or controls. Type 1 products contain classified NSA algorithms. They are available to U.S. Government users, their contractors, and federally sponsored non-U.S. Government activities subject to export restrictions in accordance with International Traffic in Arms Regulations.
5. A Type 2 product is an unclassified cryptographic equipment, assembly, or component, endorsed by NSA, for use in national security systems as defined in Title 40 U.S. Code, Section 1452.
6. The Data Encryption Standard (DES) is a cryptographic algorithm designed for the protection of unclassified data, and published by NIST in FIPS 46. Any DES implementation that was previously endorsed by NSA as meeting FS 1027, is equivalent to a Type 2 product. If already fielded, these formerly NSA endorsed DES implementations can still be used throughout their lifecycle; however new COMSEC applications must be either NSA endorsed, NIST validated, or HQ USAF/SC approved. A listing of cryptographic modules that were previously endorsed by NSA as complying to FS 1027 is included as an attachment of historical lists to the FIPS 140-1 Cryptographic Modules Validation List located at <http://csrc.nist.gov/cryptval>.
7. Information on HQ USAF/SC approved products having Air Force wide applications is located at <http://www.afca.scott.af.mil/ip>. HQ USAF/SC approves products that do not have Air Force wide application via individual correspondence.
8. Submit requests to use HQ USAF/SC approved products according to Attachment 2, Table A-2-1, Rule 3.

7. Physical Security. Physical security is that part of COMSEC which results from using all physical measures necessary to safeguard COMSEC material from access by unauthorized persons. Physical security measures include the application of control procedures and physical barriers. Apply physical security to comply with national policy requiring the U.S. government to safeguard and control COMSEC materials in a manner which assures their continued integrity, prevents access by unauthorized persons and controls the spread of COMSEC materials, techniques, and technology when not in the best interest of the U.S. and its allies. Common physical security measures include verifying the need-to-know and clearance of personnel granted access, adequate training of personnel, following proper storage and handling procedures, accurate accounting for all material, transporting via authorized means, and immediate reporting of loss or possible compromise, etc.

7.1. COMSEC Material Control System (CMCS). To further national policy to safeguard and control COMSEC materials, all COMSEC keying material is placed into the CMCS. The CMCS is a logistics and accounting system through which COMSEC material is distributed, controlled, and safeguarded. The CMCS consists of COMSEC accounts, COMSEC central offices of record, and cryptologic depots.

7.1.1. As part of the Information Assurance responsibilities outlined in AFD 33-2, *Information Protection* (to become *Information Assurance*), commanders establish COMSEC accounts necessary to support their mission. AFKAG-2, *AF COMSEC Accounting Manual*, contains procedures for establishing COMSEC accounts and provides procedures for appointing the COMSEC manager. Establish different types of COMSEC accounts as follows:

7.1.1.1. The host command for each installation with a requirement for secure information systems must establish an operational COMSEC account to support both host and tenant organization requirements.

7.1.1.2. Each headquarters that has COMSEC planning, programming, supervising, or monitoring responsibilities may establish an administrative COMSEC account.

7.1.1.3. Any organizational level may establish a mobile or contingency account where the need exists to provide COMSEC material to support activities when they are operationally deployed.

7.1.1.4. The contracting command determines whether contractor facilities requiring COMSEC material in support of an Air Force contract, must establish their own COMSEC account or receive support from the installation's existing COMSEC account. AFKAG-2, AFI 31-601, and DoD 5220.22-S, *COMSEC Supplement to Industrial Security Manual for Safeguarding Classified Information*, contain procedures for establishing Air Force contractor COMSEC accounts. If the contractor establishes their own Air Force COMSEC account, Air Force directives apply to account and user operations. If the contractor facility receives support from an existing COMSEC account, the guidance and directives applicable to the supporting COMSEC account also apply to the contractor's operations. Normally, contractors that already operate an NSA COMSEC account will use that account to support Air Force requirements.

7.1.2. Within the Air Force, HQ CPSG acts as the Central Office of Record (COR).

7.1.3. The United States National Distribution Authority (USNDA), which is operated by NSA, is the primary cryptologic depot for the distribution of COMSEC keying material, and HQ CPSG serves as the Air Force cryptologic depot for the distribution of COMSEC equipment and a limited number of COMSEC aids.

7.2. Safeguarding and Control of COMSEC Materials. AFKAG-1 and AFI 33-211 provide detailed instructions on the proper procedures to safeguard and control COMSEC materials.

7.2.1. AFKAG-1 provides detailed COMSEC safeguarding and handling instructions for COMSEC accounts.

7.2.2. AFI 33-211 implements the requirements of AFKAG-1 at the user level and provides detailed COMSEC safeguarding and handling instructions for COMSEC users.

7.3. Release of COMSEC Information to U.S. Contractors and Other U.S. Nongovernmental Sources. The government ordinarily conducts government COMSEC operations; however, national policy permits the government to obtain required COMSEC goods and services from, and provide COMSEC information and material to, U.S. nongovernmental sources, subject to certain limitations.

7.3.1. Do not release U.S. Government COMSEC information outside of the U.S. Government unless the following criteria can be met:

7.3.1.1. Ensure a valid need exists for an individual or organization to:

7.3.1.1.1. Install, maintain, or operate COMSEC equipment for the U.S. Government;

7.3.1.1.2. Participate in the design, planning, production, training, installation, maintenance, operation, logistical support, integration, modification, testing, or study of COMSEC material or techniques; or

7.3.1.1.3. Transmit classified national security information by secure means or provide protection during the transmission of sensitive information.

7.3.1.2. Grant access to classified COMSEC information only to individuals who hold a final U.S. Government security clearance for the highest classification level involved.

7.3.1.3. Ensure all individuals provided access to COMSEC information are trained regarding the unique nature of COMSEC information and their security responsibilities to properly safeguard and control it.

7.3.1.4. Ensure all individuals who maintain U.S. Government COMSEC equipment have received formal NSA-approved training on such equipment.

7.3.2. Security standards and procedures applicable to any COMSEC information released outside of the U.S. Government must in all cases be consistent with established COMSEC doctrine and the specific requirements of this paragraph. In particular:

7.3.2.1. Grant access to U.S. Government COMSEC information to only U.S. citizens. Control such access on a strict need-to-know basis and grant access only in conformance with procedures established for the particular type of COMSEC information involved. Process requests for the release of COMSEC information to U.S. individuals who are not U.S. citizens as an exception to national policy and submit according to Attachment 2.

7.3.2.2. NSA must grant specific approval when contracting for design, development, modification, production, or developmental testing of cryptographic equipment.

7.3.2.3. As a prior condition of release, control COMSEC information provided to nongovernmental U.S. persons in such a manner as to prevent its further dissemination outside of the U.S. Government or the unauthorized transfer of technology contained therein.

7.3.2.4. Comply with applicable cryptographic access policies when granting individuals access to U.S. COMSEC information. The contracting activity ensures compliance with DoD 5220.22-M, DoD 5220.22-S, AFI 31-601, and AFKAG-1 concerning security clearance requirements for contractor personnel.

7.3.3. Submit waivers to these requirements according to Attachment 2.

7.4. Release of COMSEC Products or Associated Information to Foreign Governments or International Organizations. Protect U.S. Government COMSEC products or associated COMSEC information that are used to secure national security systems as they are valuable national assets. These products and information will be released to foreign governments or international organizations only when there is a clearly defined benefit that is consistent with U.S. Government foreign policy and military or economic objectives and the release is specifically authorized by the National Security Telecommunications and Information Systems Security Committee (NSTISSC) consistent with law, regulations, Executive Orders, and applicable Presidential Directives and in accordance with the criteria limitations and procedures specified below. Submit requests to release COMSEC products or associated information to foreign governments or international organizations according to Attachment 3.

7.4.1. The NSTISSC considers requests to release COMSEC products and associated COMSEC information to a foreign government or an international organization to satisfy requirements that have been identified by the Air Force to:

7.4.1.1. Protect U.S. Government national security information which is provided to, or exchanged with, a foreign government or international organization.

7.4.1.2. Enhance the objectives and effectiveness of mutual U.S. Government defense arrangements or coalition operations by providing a means for achieving secure communications interoperability when exchanging military planning information, or conducting combined or coalition combat operations which involve U.S. Government military forces and the military forces of a foreign government(s) or international organization.

7.4.1.3. Protect U.S. Government national security information which is provided to or exchanged with a foreign government or international organization in support of U.S. Government efforts to combat the transnational threats of international crime, international terrorism, international drug trafficking, or proliferation of weapons of mass destruction.

7.4.2. Requests for release of U.S. Government COMSEC products or associated COMSEC information must:

7.4.2.1. Be consistent with U.S. Government foreign policy and military or economic objectives;

7.4.2.2. Have no unacceptable impact on U.S. Government Signals Intelligence (SIGINT) activities; and

7.4.2.3. Not impact adversely on the overall INFOSEC posture of the U.S. Government.

7.4.3. In those cases where the terms of an NSTISSC release authorization must be documented in a formal Memorandum of Understanding (MOU), the NSTISSC may provide negotiating guidelines for the Air Force. Prior to signing, the Director, National Security Agency, acting in his capacity as the National Manager for National Security Telecommunications and Information Systems Security (NSTISS), must review and approve the MOU to ensure compliance with NSTISSC release guidelines.

7.4.4. Provided the release request meets the criteria in paragraph 7.4.1. and 7.4.2., and the request has been approved, the following limitations apply to the release of COMSEC products or associated COMSEC information:

7.4.4.1. U.S. Government COMSEC products or associated COMSEC information will normally not be authorized for release solely for purposes of improving the COMSEC posture of a foreign government or international organization.

7.4.4.2. The inclusion of COMSEC products or associated COMSEC information in weapons, communications, or other major defense systems, to provide a complete package for Foreign Military Sales (FMS), or initiatives to promote international competition for system procurements, are not, in and by themselves, acceptable justifications for seeking release of those products or information.

7.4.4.3. The transfer of U.S. Government COMSEC products or associated COMSEC information will normally be accomplished on government-to-government basis through FMS channels. The National Manager for NSTISS will consider and approve, on a case-by-case basis, the use of other than FMS channels, such as providing COMSEC products, information, or services as part of arrangements with foreign countries for cryptologic support pursuant to Title 10 U.S. Code 421. As necessary, Air Force personnel will provide training to the recipients of U.S. Government COMSEC products or associated COMSEC information to ensure proper operation and protection in accordance with prescribed U.S. Government standards.

7.4.4.4. During U.S./Allied combined exercises, U.S. Government equipment, including classified and unclassified equipment handled as controlled cryptographic items (CCI), which has not been released to a foreign country, may be used provided the U.S. and allies adhere to the following procedures and controls. For the following procedures, access is defined as being limited to external exposure including use and operation of sealed COMSEC devices.

7.4.4.4.1. Foreign nationals are not permitted unaccompanied access to any U.S. government COMSEC equipment without specific NSA authorization and release by the NSTISSC. If the equipment is going to be used in a foreign owned or leased facility, plane, or ship, the controlling U.S. command must request a waiver according to Attachment 3.

7.4.4.4.2. During exercises and combined operations, foreign nationals may be authorized limited access to sealed U.S. government COMSEC equipment provided they are accompanied by appropriately cleared U.S. personnel and NSA has granted a waiver.

7.4.4.4.3. Foreign nationals may not, at any time, have access to any opened U.S. government COMSEC equipment. All units must remain fully sealed and secured at all times when foreign nationals are present.

7.4.4.4.4. Foreign nationals may not, at any time, have access to keying material for the devices. Foreign nationals may be present when CCI equipment is keyed by cleared U.S. personnel, but are not permitted to load or handle any keying material associated with the equipment.

7.4.4.4.5. 24-Hour physical control, keying, and control of key will be accomplished by appropriately cleared U.S. personnel only.

DAVID B. WARNER, Lt Col, USAF

FOR OFFICIAL USE ONLY

Chief, Information Assurance Branch
AF Communications and Information Center

FOR OFFICIAL USE ONLY

ATTACHMENT 1**REFERENCES, ABBREVIATIONS, ACRONYMS, AND TERMS*****References***

AFI 31-601, *Industrial Security Program Management*
AFI 33-203, *The Air Force Emission Security Program*
AFI 33-211, *Communications Security (COMSEC) User Requirements*
AFI 33-215, *Controlling Authorities for COMSEC Keying Material (Keymat)*
AFI 33-230, *Information Protection Assessment and Assistance Program*
AFI 63-102, *Communications-Computer Systems Security Research, Development, Test and Evaluation*
AFKAG-1, *Air Force Communications Security (COMSEC) Operations*
AFKAG-2, *AF COMSEC Accounting Manual*
AFMAN 10-401, *Operation Plan and Concert Plan Development and Implementation*
AFMAN 33-270, *Communications and Information Systems Security Glossary*
AFMAN 33-272 (S), *Classifying Communications Security, TEMPEST, and C4 Systems Security Research and Development Information (U)*
AFPD 33-2, *Information Protection*
AFSSI 3030, *Protected Distribution Systems*
AFSSI 5024, Vol I., *The Certification and Accreditation (C&A) Process*
DoDD C-5200.5 (C), *Communications Security (COMSEC) (U)*
DoD 5220.22M, *National Industrial Security Program Operating Manual*
DoD 5220.22-S, *COMSEC Supplement to Industrial Security Manual for Safeguarding Classified Information*
DoDI S-5225.1 (S), *Communications Security (COMSEC) Assistance to Foreign Governments and International Organizations (U)*
FIPS 140, *General Security Requirements for Equipment Using the Data Encryption Standard*
FIPS 140-1, *Security Requirements for Cryptographic Modules*
FS 1027, *General Security Requirement for Equipment Using the Data Encryption Standard*
NACSI 6002, *Protection of Government Contractor Telecommunications*
NCSC-1, *National Policy for Safeguarding and Control of Communications Security Material*
NCSC-2, *National Policy on Release of Communications Security Information to U.S. Contractors and Other U.S. Nongovernmental Sources*
NSD 42, *National Policy for the Security of National Security Telecommunications and Information Systems*
NTISSP No. 1, *National Policy on Application of Communications Security to US Civil and Commercial Space Systems*
NTISSP No. 8, *National Policy Governing the Release of Information Systems Security (INFOSEC) Products or Associated INFOSEC Information to Foreign Governments*
Public Law 100-235, *The Computer Security Act of 1987*

Abbreviations and Acronyms

AFCIC	Air Force Communications and Information Center
AFEKMS	Air Force Electronic Key Management System
AFI	Air Force Instruction
AFIWC	Air Force Information Warfare Center
AFMAN	Air Force Manual
AFPD	Air Force Policy Directive
AFSSI	Air Force Systems Security Instruction
CCI	Controlled Cryptographic Item
CMCS	COMSEC Material Control System
CMV	Cryptographic Module Validation
COMSEC	Communications Security
COR	Central Office of Record
COTS	Commercial, Off-The-Shelf
DES	Data Encryption Standard
DoD	Department of Defense
DRU	Direct Reporting Unit
EMSEC	Emission Security
FS	Federal Standard
FIPS	Federal Information Processing Standard
FMS	Foreign Military Sales
FOA	Field Operating Agency
HQ AETC	Headquarters, Air Force Education & Training Command
HQ AFCA	Headquarters, Air Force Communications Agency
HQ AFMC	Headquarters, Air Force Materiel Command
HQ CPSG	Headquarters, Cryptologic Systems Group
HQ USAF	Headquarters, United States Air Force
HUMINT	Human Intelligence
IA	Information Assurance (formerly Information Protection [IP])
IPAP	Information Protection Assessment and Assistance Program
JTA-AF	Joint Technical Architecture - Air Force
MAJCOM	Major Command
MOU	Memorandum of Understanding
NACSI	National COMSEC Instruction
NCSC	National Communications Security Committee
NIST	National Institute for Standards and Technology
NSA	National Security Agency
NSD	National Security Directive
NSTISSC	National Security Telecommunications and Information Systems Security Committee
NSTISSI	National Security Telecommunications and Information Systems Security Instruction
NSTISSP	National Security Telecommunications and Information Systems Security Policy
NTISSP	National Telecommunications and Information Systems Security Policy
OPR	Office of Primary Responsibility

O&M	Operation and Maintenance
PDS	Protected Distribution System
PMO	Program Management Office
RDT&E	Research, Development, Test & Evaluation
SAF	Secretary of the Air Force
SIGINT	Signals Intelligence
TMAP	Telecommunications Monitoring and Assessment Program
TRANSEC	Transmission Security
USNDA	United States National Distribution Agency

Terms

Information Systems. Any telecommunications and/or computer related equipment or interconnected system or subsystems of equipment that is used in the acquisition, storage, manipulation, management, movement, control, display, switching interchange, transmission, or reception, of voice and/or data, and includes software, firmware, and hardware.

Note: This includes automated information systems.

National Security System. Any telecommunications or information system operated by the United States Government, the function, operation, or use of which: 1. involves intelligence activities; 2. involves cryptologic activities related to national security; 3. involves command and control of military forces; 4. involves equipment that is an integral part of weapon or weapon system; or 5. is critical to the direct fulfillment of military or intelligence missions and does not include a system that is to be used for routine administrative and business applications (including payroll, finance, logistics, and personnel management applications). (Title 40 U.S.C. Section 1452, Information Technology Management Reform Act of 1996).

National Security Information (synonymous with Classified Information). Information that has been determined, pursuant to Executive Order 12958 or any other preceding order, to require protection against unauthorized disclosure.

Note: For the purpose of the above definition only, "protection" is synonymous with "securing" which is defined below.

Sensitive Information. Any information, the loss, misuse, or unauthorized access to or modification of which could adversely affect the national interest or the conduct of federal programs, or the privacy to which individuals are entitled under Section 552a of Title 5, U.S. Code (the Privacy Act), but that has not been specifically authorized under criteria established by an Executive Order or an Act of Congress to be kept secret in the interest of national defense or foreign policy.

Note: Within the Air Force, sensitive information includes, but is not limited to, information that could assist a hostile agent in developing countermeasures; involve new or high technology; or involve key indicators of operational capabilities which hostile agents could use to determine operational capabilities, weaknesses, and wartime missions.

Protection. The application of Government-approved protection equipment, devices, techniques or services to information systems over which sensitive information is transmitted.

Government-Approved Protection. Equipment or techniques that the National Security Agency (NSA) or the National Institute for Standards and Technology (NIST) determined met certain prescribed government security standards for the protection of sensitive information that is transmitted over information systems.

Securing. Applying NSA-approved COMSEC equipment, devices, techniques, or services to information systems over which classified information is transmitted.

ATTACHMENT 2

TABLE A-2-1 SUBMITTING COMSEC WAIVER REQUESTS

R U L E	A	B	C
	To request	include information from the following items of Table A-2-2	The requesting activity submits the request:
1	A waiver to COMSEC requirements for U.S. Civil and Commercial Space Systems.	1, 2, 3, 5, 8 (include the reason encryption cannot be applied), 9, 13, & 14.	to their servicing COMSEC account who forwards it to their MAJCOM Information Assurance (IA) office. The MAJCOM IA office submits it to the appropriate MAJCOM operations personnel for a technical evaluation. Based on the technical evaluation, the MAJCOM IA office evaluates the request and notifies the requesting activity of approval (along with any operational restrictions) or disapproval.
2	A waiver to requirements for the release of COMSEC information to U.S. contractors and other U.S. nongovernmental sources to include exceptions for the release requirements of COMSEC information to U.S. individuals who are not U.S. citizens.	1, 2, 4, 6, 7, 8, 10, 11, 12, 13, & 14.	to their servicing COMSEC account who forwards it to their MAJCOM Information Assurance (IA) office. The MAJCOM IA office evaluates the request, and if they concur, submits it to HQ AFCA/GCIS for further evaluation. If HQ AFCA/GCIS concurs, they will forward it to NSA for approval/disapproval. If approved, NSA will provide any operational restrictions or alternate arrangements.
3	An exception to AF requirements on the use of NSA endorsed/NIST validated products	1, 2, 3, 5, 8 (to include CSRD or ORD and technical solution), 9, 11, 13, 14, & 15.	to their servicing local Information Assurance (IA) office who forwards it to their MAJCOM IA office. The MAJCOM IA office evaluates the request, and if they concur, submits it to HQ AFCA/GCIT for technical review. If HQ AFCA/GCIT concurs, they will forward it to HQ USAF/SC for approval or disapproval.

TABLE A-2-2 INFORMATION

ITEM	TYPE OF INFORMATION
1	Identify the organization, unit or agency, etc. requesting the waiver.
2	Identify the specific provision of the paragraph for which a waiver or release is required.
3	Describe the program or project the unprotected link supports and the approval date of the program or project, if applicable.
4	Identify the number of personnel involved, names, citizenship, and level of security clearance of personnel requesting access.
5	Identify the type and classification of information to be transmitted.
6	Identify the type and classification of COMSEC information and/or material to which the individuals are requesting access.
7	Identify the COMSEC functions the nongovernmental source(s) will perform; the location(s) at which COMSEC functions will be performed; the inclusive dates for which personnel will require access to COMSEC under the provision of the contract or arrangement, and their training certification or any training required.
8	Provide the justification.
9	The requested effective date and period of time the waiver will be required.
10	Indicate whether personnel will be using keying materials marked "CRYPTO" which are held or used by Government departments and agencies. If so, indicate if consideration has been given to providing unique operational keying materials?
11	Identify what additional administrative/security measures will be implemented.
12	Identify the Government department or agency which will be responsible for assuring the security of non-governmental COMSEC operations/functions.
13	State the impact if the waiver or release is disapproved.
14	Provide any other amplifying information.
15	Provide a copy of the proposed System Security Authorization Agreement (SSAA), including the Certification and Accreditation (C & A) plan, prepared according to AFSSI 5024, Vol I., <i>The Certification and Accreditation (C&A) Process</i> .

NOTES:

1. Users must justify waivers annually. HQ AFCA reviews waivers for possible application of new COMSEC technology.
2. This information collection is exempt from licensing with an RCS number according to AFI 37-124, *The Information Collection and Reports Program*.

ATTACHMENT 3

TABLE A-3-1 SUBMITTING REQUESTS FOR RELEASE OF COMSEC TO FOREIGN GOVERNMENTS OR INTERNATIONAL ORGANIZATIONS			
R U L E	A	B	C
	To request release of	to foreign governments or international organizations, include information from all items in Table A-3-2. The requesting activity submits the request to their servicing COMSEC account who forwards it to:	NSA/I11
1	a cryptosystem, that has an Air Force controlling authority,	the controlling authority with an information copy to their MAJCOM Information Assurance (IA) office. The controlling authority evaluates the request, and provides their recommendations to HQ AFCA/GCIS who submits it to:	for evaluation, feedback, further referral, and or approval/disapproval. When NSA is the release approval authority, they will provide a recommended release solution. The requesting activity determines resource availability and identifies a proposed method of transfer (e.g. sale, lease, or loan) or works with NSA to address resource shortfalls. If the release requires NSTISSC approval, NSA refers the request through the proper channels along with their recommendations.
2	a cryptosystem, that has a controlling authority that is other than Air Force,	the controlling authority with an information copy to their MAJCOM Information Assurance (IA) office and HQ AFCA/GCIS. The controlling authority evaluates the request and has the option of either providing their recommendations to HQ AFCA/GCIS who will submit the request to NSA, or they can provide their recommendations directly to:	
3	U.S. COMSEC equipment, products, or associated information to include requests for foreign nationals to have unaccompanied access to U.S. government COMSEC equipment,	HQ AFCA/GCIS with an information copy to their MAJCOM Information Assurance (IA) office. HQ AFCA/GCIS forwards it to:	

FOR OFFICIAL USE ONLY

TABLE A-3-2 INFORMATION	
ITEM	TYPE OF INFORMATION
1	Identify the organization, unit or agency, etc. requesting the release.
2	Identify the specific provision of the paragraph for which a waiver or release is required.
3	Identify the foreign government and/or organization for which release is requested and the number of personnel and their citizenship.
4	Identify the type and classification of COMSEC information and/or material to which the individuals are requesting access and a recommended method of transfer (sale, lease, or loan).
5	Identify the COMSEC functions the foreign government or organization(s) will perform, the location(s) at which COMSEC functions will be performed; the inclusive dates of the exercise or for which personnel will require access to COMSEC under the provision of the arrangement; and their training certification or any training required.
6	Provide the justification.
7	Indicate whether personnel will be using keying materials marked "CRYPTO" which are held or used by Government departments and agencies. If so, indicate if consideration has been given to providing unique operational keying materials?
8	Identify what additional administrative/security measures will be implemented.
9	State the impact if the waiver or release is disapproved.
10	Provide any other amplifying information.

NOTE: This information collection is exempt from licensing with an RCS number according to AFI 37-124, *The Information Collection and Reports Program*.