BY ORDER OF THE SECRETARY OF THE AIR FORCE

AIR FORCE INSTRUCTION 71-101, VOLUME 4

1 AUGUST 2000

Special Investigations

COUNTERINTELLIGENCE

COMPLIANCE WITH THIS PUBLICATION IS MANDATORY

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

OPR: SAF/IGX (Maj Eugene A. Longo)

Certified by: SAF/IGX (Col Charles P. Azukas)

Pages: 7

Distribution: F

This volume implements AFPD 71-1, *Criminal Investigations and Counterintelligence*, and provides guidance for conducting counterintelligence activities. It implements DoD Instruction 5240.6, *Counterintelligence Awareness and Briefing Program*, DoD 5240.1-R, *Procedures Governing the Activities of DoD Intelligence Components That Affect United States Persons*, and DoD Instruction C-5240.8, *Security Classification Guide for Information Concerning the DoD Counterintelligence Program*. This volume authorizes the collection and maintenance of information protected by the Privacy Act of 1974. The authority to collect and maintain this information is in Title 10, United States Code (U.S.C.), Sections 8013 and 801-940. Systems of Records Notices F071 AFOSI A, *Counterintelligence Operations and Collection Records*, and F071 AFOSI C, *Criminal Records*, also apply. The instructions in this volume do not confer upon an individual any rights or privileges that applicable law does not require. See attachment 1 for the Glossary of References and Supporting Information.

Records Disposition. The reporting requirement in this instruction is exempt from licensing in accordance with Paragraph 2.11.1 of AFI 37-124, *The Information Collections and Reports Management Program; Controlling Internal, Public, and Interagency Air Force Information Collections*. Maintain and dispose of all records created by processes prescribed in this instruction IAW AFMAN 37-139, *Records Disposition Schedule*.

1. Counterintelligence. The Air Force Office of Special Investigations (AFOSI) initiates and conducts all counterintelligence investigations, operations, collections, and other related activities for the Air Force.

1.1. In the United States, AFOSI coordinates when appropriate, these activities with the Federal Bureau of Investigations (FBI).

1.2. Outside the United States, AFOSI coordinates when appropriate, these activities with the Central Intelligence Agency (CIA) and the FBI as appropriate.

2. Counterintelligence Awareness and Briefing Program. Air Force commanders will ensure their personnel are briefed on the counterintelligence threat that foreign intelligence services (FIS) pose and on the requirements of this instruction.

2.1. Air Force commanders should seek to instill in their personnel a high level of awareness of the threat to classified, sensitive, and proprietary information from foreign sources, as well as from inadvertent or deliberate disclosures by cleared personnel.

2.2. Military personnel must receive recurring awareness briefings upon permanent change of station or every three years- whichever is less.

2.2.1. Civilian employees must receive recurring briefings at least every three years.

2.2.2. The Air Education and Training Command (AETC) provides military members with their initial awareness briefing during basic training or pre-commissioning programs.

2.2.3. Air Force commanders ensure that military personnel entering the Air Force directly, through means other than AETC, and all civilian personnel receive the briefing during their initial assignment.

2.3. AFOSI is the installation-level training agency for Counterintelligence Awareness briefings.

2.4. Other defense components accessing or employing military and civilian personnel must brief them according to DoD Directive 5240.6, *Counterintelligence Awareness and Briefing Program*, July 16, 1996.

2.5. Trainers should tailor the briefing for the audience, but every briefing should include:

2.5.1. The threat posed by foreign intelligence, foreign government-sponsored commercial enterprises, all pertinent terrorist threats, and international narcotics trafficking organizations.

2.5.2. The threat to the specific installation or mission.

2.5.3. Specific security vulnerabilities of the Major command.

2.5.4. A discussion of how the threat specifically applies to the installation and the individuals' responsibilities.

2.5.5. The reporting requirements of this instruction.

2.6. The following persons are required to report incidents IAW paragraph 2.1.7. All other persons associated with Air Force activities but not listed below should be encouraged to report counterintelligence incidents.

2.6.1. Active duty Air Force personnel and Air Force civilian employees.

2.6.2. US Air Force Reserve personnel while in active status and Category B reservist's on inactive duty for training (IDT) status.

2.6.3. Air National Guard personnel when federalized.

2.6.4. Foreign national employees of the DoD in overseas areas, as stipulated in command directives and the Status of Forces Agreements (SOFA).

2.6.5. Contract employees and DoD contractor employees when specified in their contract.

2.6.6. Civilian employees of US defense agencies (except the Defense Intelligence Agency) for which AFOSI provides counterintelligence support in accordance with DoD 5240.6 (see DoD 5240.6 Enclosure #3 for the list of DoD agencies AFOSI is the designated counterintelligence executive agent) and the overseas employees of the US government for whom the Air Force provides either administrative or logistical support under DoD 5240.6.

2.7. AFOSI is the sole Air Force repository for the collection and retention of reportable information as described below. Individuals who have reportable contacts or acquire reportable information must immediately (within 30 days of the contact) report the contact or information, either verbally or in writing, to AFOSI. If necessary, the individual can report the information to his/her commander, supervisor, or security officer who must immediately provide the information to their servicing AFOSI detachment. For the purpose of this paragraph "contact" means any exchange of information directed to an individual including solicited or unsolicited telephone calls, e-mail, radio contact, etc., in addition to face-to-face meetings. It does not include contact by "mass media" such as television or radio broadcasts, public speeches or other means not directed at specific individuals. It also does not include contact as part of the official duties of the member, however nothing in this paragraph replaces or eliminates reporting required as part of official duties.

2.7.1. Personal contact with an individual (regardless of nationality) who suggests that a foreign intelligence or any terrorist organization may have targeted them or others for possible intelligence exploitation.

2.7.2. A request by anyone (regardless of nationality) for illegal or unauthorized access to classified or unclassified controlled information.

2.7.3. Contact with a known or suspected intelligence officer to include attachés from any country.

2.7.4. Contact for any reason, other than for official duties, with a foreign diplomatic establishment, whether in the United States or abroad. **NOTE:** Certain Air Force members and civilian employees in positions designated as "sensitive" by their Air Force component also may be required to notify their commanders or supervisors in advance of the nature and reason for contacting a foreign diplomatic establishment.

2.7.5. Activities related to planned, attempted, actual, or suspected espionage, terrorism, unauthorized technology transfer, sabotage, sedition, subversion, spying, treason, or other unlawful intelligence activities targeted against the Department of the Air Force, other US facilities, organizations, or US citizens.

2.7.6. Information indicating military members, civilian employees or DoD contractors have contemplated, attempted, or effected the deliberate compromise or unauthorized release of classified or unclassified controlled information.

2.7.7. Unauthorized intrusion into US automated information systems, whether classified or unclassified; unauthorized transmissions of classified or unclassified controlled information without regard to medium, destination, or origin.

2.7.8. Unauthorized attempts to bypass automated information systems security devices or functions, unauthorized requests for passwords, or unauthorized installation of modems or other devices into automated information systems (including telephone systems) whether classified or unclassified.

3. Sanctions. DoD, Air Force or contractor personnel who fail to report information required by this instruction may be subject to judicial and/or administrative action under applicable law and instructions, including the Uniform Code of Military Justice, 10 U.S.C. 801-949, and other applicable sections of the United States Code.

4. Classifying Counterintelligence Information. Except for information subject to the Atomic Energy Act of 1954 (as amended), AFOSI assigns classification markings to counterintelligence information according to the guidelines in DoD 5200.1-R, *Information Security Program*, DOD Instruction 5240.8, *Security Classification Guide for Information Concerning the DoD Counterintelligence Program*, and Executive Order 12958, *Classified National Security Information*. These publications and executive order provide the only basis for application of security classification to counterintelligence information within the DoD.

5. Acquiring Intelligence Information about US Persons. Information about a US Person (see attachment 1 for the definition of US Person), may be collected by AFOSI in its role as a designated counterintelligence component only if it is necessary to perform its assigned mission. The collection and/or retention must meet the standard of information that can be collected or retained as defined by Procedures 2 and 3 of DoD 5240.1-R, *Procedures Governing the Activities of DoD Intelligence Components that Affect US Persons*, which are incorporated by reference.

6. Use of Specialized Techniques in Counterintelligence Investigations and Operations:

6.1. AFOSI is the sole agency within the Air Force authorized to use specialized techniques, as defined in Procedures 5 through 10, DoD 5240.1-R, in counterintelligence activities, or to request other agencies to conduct these techniques in support of the Air Force. For the purposes of this paragraph, AFOSI is a DoD intelligence component as defined in DoD 5240.1-R.

6.1.1. Unless otherwise proscribed by law, specialized techniques may be authorized by the appropriate approving authority for a period of 90 days. Extensions can be granted upon submission of appropriate justification. All requests and approvals will be documented in internal AFOSI records and will be disclosed only to authorized agencies for official purposes.

6.1.2. The procedures described below are applicable only upon determination by HQ AFOSI that the activity is for counterintelligence purposes. In all other AFOSI activities the procedures prescribed in AFI 71-101 Volume 1, *Criminal Investigations*, will apply.

6.1.3. Requests for all other specialized techniques, supporting counterintelligence activities, not covered in this instruction will be forwarded to HQ AFOSI where the appropriate approval level will be ascertained.

6.1.4. The Commander, AFOSI, will publish internal instructions directing the conduct and approval process for all techniques under this paragraph. AFOSI will document the approvals, the specific techniques utilized, the identity of persons monitored, and the disposition of the products of such monitoring in internal documentation.

6.1.5. In joint investigations, AFOSI may utilize specialized techniques under the approval authority of another authorized US federal agency (normally FBI) after consultation with HQ AFOSI/JA.

6.2. US Persons. The use of specialized techniques in counterintelligence activities involving US persons is governed by DoD 5240.1-R. The Office of the Staff Judge Advocate, AFOSI, will review, in writing, each request to ensure it complies with Intelligence Oversight policy.

6.2.1. Procedures requiring approval outside AFOSI will be staffed through HQ AFOSI to SAF/GC. The request will be reviewed by SAF/GC who will ensure approval is obtained from the appropriate authority.

6.2.2. The Commander, AFOSI may approve the use of physical, photographic or video surveillance activities supporting the counterintelligence mission that are not within the purview of Procedure 5, Electronic Surveillance, DoD 5240.1-R

6.2.3. The Commander, AFOSI, after coordination with the SAF/GC, may approve the acquisition of nonpublic wire, oral or electronic communications where at least one party to the communication consents to such acquisition. In emergency situations, the activity may be approved after consultation with HQ AFOSI/JA. In such cases coordination with SAF/GC must occur within 48 hours after the approval.

6.3. Non-US Persons Within the US. Request for the use of specialized techniques in counterintelligence activities targeting non-US persons within the United States will be sent to HQ AFOSI/JA where the appropriate level of approval will be ascertained.

6.4. Non-US Persons Outside the United States. The use of specialized techniques in counterintelligence activities targeting non-US persons outside the United States may be subject to Status of Forces Agreements (SOFA) and will be coordinated and approved in accordance with the Director Central Intelligence Directive 5/1, *Espionage and Counterintelligence Activities Abroad* in addition to the approvals below. In deployed areas, the supporting SJA will also review the application of each technique to ensure compliance with Intelligence Oversight policy and/or the Law of Armed Conflict (LOAC).

6.4.1. The Commander, AFOSI may approve the use of physical, photographic or silent video surveillance activities supporting the counterintelligence mission outside the United States, which are targeting non-US persons. This authority may be delegated to subordinate AFOSI Commanders and/or senior special agents supporting deployed Air Force contingents.

6.4.2. The Commander, AFOSI may approve the interception of wire, oral or electronic communications targeted against non-US persons where all US persons involved are knowledgeable and consent to the monitoring. This authority may be delegated no lower than AFOSI Region Commanders.

NICHOLAS B. KEHOE, Lt General, USAF
The Inspector General

Attachment 1

GLOSSARY OF REFERNCES AND SUPPORTING INFORMATION

References

Executive Order 12958, *Classified National Security Information,* April 1995

AFPD 71-1, *Criminal Investigations and Counterintelligence*

DoD Directive 5240.2, *DoD Counterintelligence*, 22 May, 1997

DoD Instruction 5240.6, *Counterintelligence Awareness and Briefing Program,* 16 July 1996

DoD 5240.1-R, *Procedure Governing the Activities of DoD Intelligence Components That Affect United States Persons,* December 1982

DoD Instruction C-5240.8, *Security Classification Guide for Information Concerning the DoD Counterintelligence Program,* 8 March 1987

Director of Central Intelligence Instruction (DCID) 5/1, *Espionage and Counterintelligence Abroad,* 19 December, 1984

Title 10, United States Code (U.S.C.), Section 8013

Title 10, U.S.C. 801-940

Systems of Records Notices F071 AF OSI A, *Counterintelligence Operations and Collection Records* and F071 AF OSI C, *Criminal Records*

Public Law 95-511, *Foreign Intelligence Surveillance Act of 1978*

DoD 5240.6, CI Awareness and Briefing Program

Terms

Classified National Security Information—Information that has been determined pursuant to Executive Order 12958 or any predecessor Executive Order, to require protection against unauthorized disclosure and is marked to indicate its classified status when in document form.

Contact—Any form of meeting, association, or communication, in person, by radio, telephone, letter or other means, regardless of who started the contact or whether it was for social, official, private, or other reasons.

Counterintelligence (CI)—Information gathered and activities conducted to protect against espionage, other intelligence activities, sabotage, or assassinations conducted by or on behalf of foreign governments or elements thereof, foreign organizations or foreign persons, or international terrorist activities.

Electronic Surveillance—Acquisition of nonpublic communication by electronic means without the consent of a person who is party to an electronic communication or in the case of a non-electronic communication, without the consent of a person who is visibly present at the place of communication, but not including the use of radio direction finding equipment solely to determine the location of the transmitter. (Electronic surveillance within the United States is subject to the definition in the Foreign Intelligence Surveillance Act of 1978.)

Foreign Diplomatic Establishment—Any embassy, consulate, or interest section representing a foreign

country.

Foreign Interest—Any foreign government, agency of a foreign government, or representative of a foreign government; any form of business enterprise or legal entity organized, chartered, or incorporated under the laws of any country other than the United States, or its possessions and trust territories; and any person who is not a citizen or national of the United States.

Military Department CI Agency and DoD CI Agency—The military department CI agencies include Army Counterintelligence, the Naval Criminal Investigative Service and the Air Force Office of Special Investigations. DoD CI agencies include the foregoing plus the CI elements of the Defense Intelligence Agency, Defense Security Service, National Reconnaissance Office, National Security Agency, and Defense Threat Reduction Agency.

Technology Transfer—The export of controlled technical information, data, and/or material to a foreign interest pursuant to 50 App. U.S.C. 2401, and 22 U.S.C 2751.

Terrorism—The calculated use of violence or threat of violence to inculcate fear intended to coerce or to intimidate governments or societies in the pursuit of goals that are generally political, religious, or ideological.

Unclassified Controlled Information—Information other than classified information that requires application of controls and protective measures because the information is exempt from release under the Freedom of Information Act. Examples include “For Official Use Only” information, “Sensitive but Unclassified” (Formerly “Limited Official Use”) information, “DEA Sensitive Information,” “DoD Unclassified Controlled Nuclear Information,” or “Sensitive Information” as defined in the Computer Security Act of 1987, and information contained in Technical Documents.

US Persons—

(a) The term “United States Person” applies to the following:

(1) A United States citizen.

(2) An alien known by the DoD intelligence component concerned to be a permanent resident alien. A permanent resident alien is a foreign national lawfully admitted into the United States for permanent residence.

(3) An unincorporated association substantially composed mostly of United States citizens or permanent resident aliens.

(4) A corporation incorporated in the United States, except for a corporation directed and controlled by a foreign government or governments.

(b) The term “Non-US Person” applies to the following:

(1) A corporation or corporate subsidiary incorporated abroad even if partially or wholly owned by a corporation incorporated in the United States.

(2) A person or organization outside the United States unless specific information to the contrary is obtained.

(3) An alien in the United States unless specific information to the contrary is obtained.

Unofficial Contact—Contact not specifically required in accordance with job responsibilities.