BY ORDER OF THE
SECRETARY OF THE AIR FORCE

AIR FORCE INSTRUCTION 14-302

18 JANUARY 1994

Intelligence

CONTROL, PROTECTION, AND DISSEMINATION OF SENSITIVE COMPARTMENTED INFORMATION

COMPLIANCE WITH THIS PUBLICATION IS MANDATORY

OPR: 497 IG/INSC (Elizabeth A. Hall)

Certified by: 497 IG/INS (Col Michael R. Hollomon)

Supersedes AFR 200-7, 16 October 1992; and AFR 205-19

Pages: 8

Distribution: F

This instruction implements AFPD 14-3, *Control, Protection, and Dissemination of Intelligence Information,* AFMAN 14-304, *The Security, Use, and Dissemination of Sensitive Compartmented Information (U),* Director of Central Intelligence Directive (DCID) 1/19, *DCI Security Policy Manual for SCI Control System,* and DCID 1/21, *DCI Manual for Physical Security Standards for SCI Facilities,* and explains Air Force rules, responsibilities, and terminology for the security, use, and dissemination of Sensitive Compartmented Information (SCI). It also describes the functions and responsibilities assigned to Air Force senior intelligence officers (SIO), SCI security officials, communications security (COMSEC) managers and custodians who are SCI indoctrinated, and commanders and supervisors of SCI-indoctrinated individuals.

This instruction requires the collection and maintenance of information to be protected by the Privacy Act of 1974. The authority to collect and maintain this information is in Executive Order 12333, *United States Intelligence Activities*. System of records notice F205 497 IG/INS applies.

SUMMARY OF REVISIONS

This revision aligns the instruction with AFPD 14-3.

1. Functions of the Air Force SCI Security Program and the Special Security Officer (SSO) System.

1.1. The SCI Security Program gives the Air Force an exclusive, responsive, and secure means to receive, store, send, use, and protect SCI. The program assists individuals working with SCI material to avoid its compromise and ensure its dissemination to appropriate personnel. It also protects SCI information from interference by uncleared and unauthorized personnel and means

1.2. The SSO System protects sources and methods, while permitting those with a valid need-to-know to receive intelligence information.

2. SCI Responsibilities. AFMAN 14-304 provides complete and detailed responsibilities.

2.1. Assistant Chief of Staff, Intelligence (ACS/I), HQ USAF. The Air Force Senior Official of the Intelligence Community (SOIC). Implements and carries out the Director of Central Intelligence (DCI) policies and procedures for protecting, using, and disseminating SCI.

2.2. IG/INS, Directorate of Security and Communications Management. Appointed by ACS/I to exercise ACS/I SCI security authority. Interprets all Intelligence Community (IC) SCI policy for the Air Force and issues management guidance.

2.3. Senior Intelligence Officer (SIO). SIOs (major command [MAJCOM] and unit) exercise overall management of SCI programs and that portion of the Special Security Office system under their control. SIOs will:

- Establish an agreement or requirement with the supporting Air Force communmications element to ensure SCI security, timely communications support to the intelligence mission, and privacy communications support.
- Identify communications-electronics (C-E) and COMSEC needs to the supporting communications element commander.
- Place the SSO in the organization so the SIO writes the SSO's performance report.
- Ensure commanders comply with responsibilities in paragraph **2.5.** and report all personnel data that pertains to SCI-indoctrinated individuals to 497 IG/INS as required by AFMAN 14-304.
- Keep the SSO informed of any issue that surfaces at the base Facilities Utilization Board, the Communications-Computer Systems Requirements Board, the Base Security Council, and similar forums which might have SCI implications.

2.4. Special Security Officer (SSO). Each SSO has day-to-day responsibility and SCI security cognizance for the parent unit, supported and subordinate organizations, and subordinate SCI facilities (SCIF). SSOs are directly responsible to the SIO and will:

- Ensure SCI is sent only to authorized persons who have a verified need-to-know.
- Ensure all individual positions which require SCI access are "S" coded by unit manpower in the unit manning document (UMD) and in the Automated Personnel Data System according to AFMAN 36-2622, volume 1, *Base Level Military Personnel System* (formerly AFM 30-130).
- Retain SCI security cognizance of the Defense Special Security Communications System (DSSCS) Telecommunications Center (TCC) or Consolidated Telecommunications Center (CTCC), and interface with the TCC and Automated Information System (AIS) facilities to ensure proper SCI security and service to the SIO.
- Provide privacy communications support to flag officers residing on or transiting through the base, and to other senior officers as requested.

2.5. All Commanders and Supervisors. Commanders and supervisors of SCI-indoctrinated personnel must provide changes in personal status to the SSO. Examples of these changes include any

arrests, disciplinary actions, letters of counseling or reprimand, Article 15 actions, incidents involving alcohol or drug abuse, etc.

2.6. Director, Base Medical Service. The medical community will give commanders and SSOs information about a person's continued eligibility for SCI access and information about treatment which may temporarily affect an SCI-indoctrinated individual's ability to perform sensitive duties. Detail specific responsibilities of the director, base medical service in a memorandum of agreement.

2.7. Chief, Security Police. The chief, security police, will provide physical protection support for approved SCIFs and, according to AFI 31-209, *Air Force Resource Protection Program,* AFPD 31-4, *Information Security*, AFPD 31-5, *Investigations, Clearances, and Program Requirements,* AFI 31-101, *Air Force Physical Security Program* ,and AFMAN 14-304, will:

- Establish procedures for security teams to respond to SCIF alarms in a timely manner.
- Allow the unit commander, SSO, or designated representative access to daily blotter inputs which may affect the continued eligibility of SCI-indoctrinated personnel.
- Establish the SCIF as a controlled area as specified in AFI 31-209 or, if justified by mission, establish a restricted area and protect it according to AFI 31-101.

2.8. Base TEMPEST Officer and Noncommissioned Officer (NCO). While the ACS/I, through 497 IG/INS, is the TEMPEST authority for SCIFs, base TEMPEST officers and NCOs have certain responsibilities. They will ensure equipment and systems are installed according to TEMPEST criteria and conduct annual RED/BLACK inspections. AFI 33-220, *TEMPEST Countermeasures Assessments and Applications,* and AFMAN 14-304 specify base TEMPEST officer and NCO responsibilities.

2.9. Base Civil Engineer:

- Construct or modify all facilities designated as SCIFs according to DCID 1/21 standards, unless waived by 497 IG/INS.
- Ensure all requests for SCI-level shielded enclosures include: 1) National Telecommunications and Information Systems Security Instruction 7000 analysis; 2) Analysis accomplished with the coordination of the host base or MAJCOM TEMPEST officer; 3) A letter or message from 497 IG/INS stating the shielded enclosure is necessary for the proposed SCIF.
- Handle requests for assistance on security-related problems in SCIFs on a priority basis.

2.10. Supporting Communications Element:

- Operate and maintain dedicated intelligence communications systems and CTCCs to provide timely intelligence communications support.
- Provide C-E and COMSEC programming for communications according to the supported unit's validated requirements.
- Maintain the Communications-Electronics Authorization Program for TCCs.
- Ensure TCC personnel are trained and qualified in all aspects of DSSCS operating procedures.
- Implement approved communications plans and programs.
- Appoint properly cleared COMSEC officers and custodians.
- Provide resources, on a rapid response basis, to meet the needs for communications service during peak activities, catastrophes, or fluctuations in the intelligence mission. Provide these

resources according to priorities established in the circuit restoration priority list or other authoritative source, such as a MAJCOM operations plan or local directive.

3. SCI Security Incidents and Violations:

3.1. Immediately report incidents involving possible compromise or improper handling of SCI material to the closest SSO. Security police personnel, unless they are an SSO, are not authorized to investigate SCI security incidents or violations.

3.2. The SSO will report, initiate, and ensure inquiry officers conduct inquiries or investigations and prepare reports on SCI security incidents, except those referred to the Air Force Office of Special Investigations or the Federal Bureau of Investigation. The SSO will remain the office of primary responsibility until the cases are formally closed. SSOs are the focal point for other investigative agencies involved in the SCI security incidents. Contractor SSOs will report and investigate SCI security incidents in the same way as Air Force SSOs (Department of Defense [DoD] 5220.22-M, *Industrial Security Manual for Safeguarding Classified Information,* January 1991).

3.3. Unlike security violations reported under AFPD 31-4, SCI violations cannot be closed by the local commander. All cases must be reviewed and closed at least by the MAJCOM SSO and in most cases by 497 IG/INS or Defense Intelligence Agency (DIA).

4. Personnel Security:

4.1. Single Scope Background Investigation (SSBI) or SSBI-Periodic Reinvestigation. See AFPD 31-5.

4.2. Due Process Procedures for SCI Eligibility Denials or Revocations. 497 IG/INS notifies each individual, through his or her commander, when denying or revoking SCI eligibility. The notice includes the reasons for denial or revocation, explains how the person may request releasable portions of applicable investigative reports, and advises that the decision may be appealed. The individual must acknowledge receipt of this notification within 5 workdays of receipt and has 45 calendar days from the date of the acknowledgment to file an appeal. If the appeal is denied by the Director, 497 IG/INS, the individual has 30 calendar days from the date of the denial letter to request review of his or her SCI eligibility disapproval by the ACS/I. The ACS/I's determination is final and not reviewable.

4.3. " **For Cause" Actions--Persons Being Considered for Court-Martial, Involuntary Separation, Discharge, or Dismissal.** When considering involuntary separation from the Air Force, dismissal from civilian employment with the Air Force, or court-martial (general or special) of an SCI-indoctrinated person, take only investigative or administrative actions until the final proposed action has been reviewed and approved by 497 IG/INS. Processing procedures for "For Cause" cases are contained in AFPD 31-5 and AFMAN 14-304.

5. Access to SCI. Personnel requiring access to SCI must have an SSBI. Additionally, the 497 IG/INS must approve indoctrination of all persons needing access to SCI.

6. Physical Security. Personnel must protect the SCIF as a controlled area or as an Air Force priority resource depending on the mission. Before accreditation is complete, the Base Security Council will review mission requirements and address physical protection. Include a copy of the security council recommendations in the accreditation package.

7. SSO Staffing. Due to the complexity of SCI security management responsibilities and requirements, minimum staffing for each SSO is three personnel. Local SIOs should justify requests for exceptions or waivers to this policy in writing to 497 IG/INS, through the MAJCOM SIOs who will add their recommendations.

8. COMSEC Keying Material. Special marking and administrative controls normally associated with SCI documentation do not apply to COMSEC keying material. See AFKAG 1, *Air Force Communications Security (COMSEC) Operations.*

ERVIN J. ROKKE, Maj General, USAF
Assistant Chief of Staff, Intelligence

Attachment 1

GLOSSARY OF REFERENCES, ABBREVIATIONS, ACRONYMS, AND TERMS

Section A--References

NOTE: If you use this instruction, you are responsible for verifying the currency of the cited references.

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

AFPD 14-3, *Control, Protection, and Dissemination of Intelligence Information*

AFMAN 14-304, *The Security, Use, and Dissemination of Sensitive Compartmented Information (U).* Formally USAFINTEL 201-1. Limited distribution through SSO channels only.

AFI 31-101, *Air Force Physical Security Program*

AFI 31-209, *Air Force Resource Protection Program*

AFPD 31-4, *Information Security*

AFPD 31-5, *Investigations, Clearances, and Program Requirements*

AFI 33-220, *TEMPEST Countermeasures Assessments and Applications*

AFMAN 36-2622, volume1, *Base Level Military Personnel System*

DCID 1/19, *DCI Security Policy Manual for SCI Control System*

DCID 1/21, *DCI Manual for Physical Security Standards for SCI* Facilities

DoD 5220.22-M, *Industrial Security Manual for Safeguarding Classified Information*

E.O. 12333, *United States Intelligence Activities*

NTISSI 7000, *National Telecommunications and Information Systems Security Instruction 7000*

Section B--Abbreviations and Acronyms

ACS/I—Assistant Chief of Staff, Intelligence

AFKAG—Air Force Cryptographic Aid General

AIS—Automated Information System

BCE—Base Civil Engineer

C-E—Communications-Electronics

COMSEC—Communications Security

CRITICOMM—Critical Intelligence Communications

CTCC—Consolidated Telecommunications Center

DISA—Defense Information Systems Agency

DCI—Director of Central Intelligence

DCID—Director of Central Intelligence Directive

DSSCS—Defense Special Security Communications System

IC—Intelligence Community

MAJCOM—Major Command

NFIB—National Foreign Intelligence Board

SCI—Sensitive Compartmented Information

SCIF—Sensitive Compartmented Information Facility

SIO—Senior Intelligence Officer

SOIC—Senior Officials of the Intelligence Community

SSBI—Single Scope Background Investigation

SPINTCOMM—Special Intelligence Communications

SSO—Special Security Office or Officer

TCC—Telecommunications Center

UMD—Unit Manning Document

Section C--Terms Explained

Defense Special Security Communications System (DSSCS).—A specialized segment of the Defense automatic digital network (AUTODIN) communications system which is operationally controlled by the Defense Information Systems Agency (DISA) and consists of automatic switching centers and interswitch trunks. DSSCS has two elements, the Critical Intelligence Communications (CRITICOMM) System and the Special Intelligence Communications (SPINTCOMM) Network. CRITICOMM is a special purpose communications network established for transmitting critical intelligence. SPINTCOMM is the communications network established for transmitting and handling SCI and other sensitive or privacy information.

Senior Intelligence Officer (SIO).—At activities below HQ USAF, the highest ranking individual charged with direct foreign intelligence missions, functions, and responsibilities within a component, command, or element. For air component commands of the unified commands and Air Force major commands, the individual must serve in a colonel or above intelligence position. If an Air Force organization has a limited or no intelligence mission or function, but requires sensitive compartmented information (SCI), the commander designates a senior officer as the SIO for SCI purposes.

Senior Officials of the Intelligence Community (SOIC).—Heads of departments and agencies within the intelligence community or their designated representatives who are senior principals and observers to the National Foreign Intelligence Board (NFIB). The Assistant Chief of Staff, Intelligence, HQ USAF, is the Air Force SOIC. For purposes of expediency and practicality, SOICs may delegate their authority to other persons within their organizations.

Sensitive Compartmented Information (SCI).—Classified information concerning or derived from intelligence sources, methods, or analytical processes, which is required to be handled exclusively within formal access control systems established by the Director of Central Intelligence (DCI).

Sensitive Compartmented Information Facility (SCIF).—A formally accredited area, room, group of rooms, or installation where SCI may be stored, used, discussed, or electrically processed. A SCIF may be permanent or temporary, mobile or fixed, and of varied construction. Procedural and physical

measures must prevent the free access of persons unless they have been formally indoctrinated for that particular SCI material authorized for use or storage within the SCIF. SCIFs are located at US Governmentcontrolled facilities, contractor plants, or other civilian locations.

Sensitive Compartmented Information Security Officials.—A generic term for those individuals appointed to positions specifically responsible for security management and control of SCI. SCI security officials include special security officers (SSO), SCI security officers, secure vault area custodians, contractor special security officers, and others. See AFMAN 14304 for appointment criteria and complete listing of duties and responsibilities for these positions.

Special Security Officer (SSO) System.—The system through which the Director, Defense Intelligence Agency (DIA), the Military Department SOICs, Air Force supported unified and specified commands, and major command SIOs perform their responsibilities for the security, use, and dissemination of SCI by both physical and electrical means. The acronym SSO is used to refer to both the office and the officer.

TEMPEST.—A short name referring to investigations and studies (e.g., TEMPEST tests, TEMPEST inspections) of compromising emanations. It is sometimes used synonymously for the term "compromising emanations."