DEPARTMENT OF THE AIR FORCE
Headquarters US Air Force
Washington DC 20330-5000

AF REGULATION 200-7

14 April 1987

Intelligence

SENSITIVE COMPARTMENTED INFORMATION (SCI) SECURITY SYSTEM

This regulation explains Air Force policy, rules, and responsibilities for the security, use, and dissemination of SCI. Together with United States Air Force Intelligence (USAFINTEL) 201-1 (binding as a standard Air Force Regulation, per AFR 8-3), it implements DOD C-5105.21-M-1, DOD TS-5105.21-M-2, and Defense Intelligence Agency (DIA) Manuals 50-3, 50-4, 50-5. It applies 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. It also applies to US Air Force Reserve and Air National Guard. See USAFINTEL 201-1, AFM 11-1, and JCS Publication 1 for a more detailed explanation of these and other terms used by the intelligence community (IC).

1. Terms Explained:

a. Defense Special Security Communications System (DSSCS). A specialized segment of the defense AUTODIN communications system which is operationally controlled by the Defense Communications Agency and consists of automatic switching centers and inter-switch 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 of SCI and other sensitive or privacy information.

b. Emergency Reaction Air Force Special Security Office (ERAFSS0). A temporary facility maintained, staffed, and operated to support operational or emergency requirements approved by HQ USAF to sustain major commands or Air Force supported unified and specified commands. May be fixed, mobile, or transportable.

c. 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 of an intelligence community organization. For air component commands of the unified commands and Air Force major commands, this individual must be serving in a colonel or above intelligence position. If an Air Force organization has a limited or no intelligence mission or function, but requires SCI, the commander designates a senior officer as the SIO for SCI purposes.

d. Senior Officials of the Intelligence Com-

Supersedes AFR 200-7, 28 June 1982. (See signature page for summary of changes.)
No. of Printed Pages: 10
OPR: INS (Lt Col John R. Reale)
Approved by: Col William C. Cody
Writer-Editor: R. M. Downey
Distribution: F

munity (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 authorities to other persons within their organizations.

e. 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).

f. 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 government-controlled facilities, contractor plants, or other civilian locations.

g. Sensitive Compartmented Information Security Officer (SCISO). The designated individual with SCI security responsibility for a SCIF. The SCISO must ensure day-to-day compliance with SCI personnel, information, physical and communications security criteria within the SCIF.

h. 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 (SCISO), secure vault area (SVA) custodians, contractor special security officers (CSSO), among others. See USAFINTEL 201-1 for appointment criteria and complete listing of duties and responsibilities of these positions.

i. Special Security Officer (SSO) System. The system through which the Director, DIA, the military departments' SOICs, Air Force-supported unified and specified commands, and major command SIOs perform their responsibilities for the security, use, and dissemination of SCI to include both physical and electrical means. The acronym SSO is used to refer to both the office and the officer.

2. Functions of the Air Force SCI Security Program and the SSO System. This program, based on the Air Force SSO System, gives the Air Force an exclusive, responsive, and secure means to receive, store, send, use, and protect SCI. It was developed to avoid compromise of SCI and guard against information denial or deception. This system protects sources and methods, while permitting the dissemination of intelligence to those with a valid need-to-know.

a. The SCI control system protects activities and information of extraordinary sensitivity. It depends on distinctive markings, restricted handling of material, stricter personnel security criteria, and protection of SCI material in "control centers" with physical and procedural barriers to preclude access by those who have not been formally approved for access. This system provides an organized method for determining need-to-know regarding specific categories of intelligence and the sources and methods employed in their collection.

b. Because of the vulnerabilities and susceptibilities of SCI systems and programs, few risks are tolerable and special judgment must be made. Individuals who have been granted TOP SECRET clearances may be denied approval for access to SCI, a direct reflection of the higher order of security afforded SCI.

c. In accepting SCI, the recipient also accepts the accompanying responsibilities and restrictions. Each individual approved for access is indoctrinated on the extreme vulnerabilities of the collection systems, the risk to the system of the unauthorized disclosure of the information they collect, and the rules for safeguarding SCI. As a condition of access, the newly approved individual signs an agreement before receiving this indoctrination briefing accepting the legal obligation to follow specific SCI security regulations and procedures.

d. The Air Force SCI security program is based on SCI policy issued by the DCI in DCI Directive (DCID) 1/19, through the Deputy Under Secretary of Defense (Policy) (DUSD(P)) and the Director, DIA.

e. Within the Air Force, the Directorate of Security and Communications Management (HQ USAF/INS) issues all SCI policy and management guidance.

f. The SSO at each Air Force command level is the single point for the receipt, control, and accountability of SCI and for SCI security

management functions for local SCIFs.

3. **SCI Responsibilities.** The more important SCI responsibilities follow. USAFINTEL 201-1 provides complete and detailed responsibilities and instructions for SCI security program functions.

a. Assistant Chief of Staff, Intelligence, HQ USAF (ACS/I). As the Air Force SOIC, the ACS/Intelligence, HQ USAF, implements and carries out within the Air Force the DCI and DOD policies and procedures of the SCI security program for the protection, use, and dissemination of SCI.

b. Directorate of Security and Communications Management (HQ USAF/INS). The ACS/I has designated the Director, Directorate of Security and Communications Management, to exercise his SCI security authority. In this capacity, HQ USAF/INS:

(1) Establishes SCI policy and procedures for the Air Force in USAFINTEL 201-1.

(2) Provides management and oversight for the Air Force SCI security program (information, personnel, physical, communications, and TEMPEST security).

(3) Prescribes policy, procedures, and responsibilities for inspection of SCI security management programs and SCIFs accredited by the Air Force. Conducts HQ USAF inspections of these programs and facilities.

(4) Determines and monitors SCI need-to-know and approves access eligibility for Air Force personnel and for contractors and consultants working on all Air Force contracts.

(5) Validates the requirement for and accredits SCIFs and communications systems in SCIFs under ACS/I, HQ USAF, security cognizance.

(6) Staffs "For Cause" discharge cases (see paragraph 4e).

(7) Develops an SCI Security Education, Awareness, and Training Program.

(8) Reviews and closes out SCI security investigations.

c. Senior Intelligence Officer (SIO). Each SIO (major command (MAJCOM) and unit) exercises overall management of SCI programs and that portion of the SSO system under his or her cognizance, except as shown in j and k below. Each SIO must:

(1) Appoint in writing all SCI security officials and alternates for organizations, SCIFs, and automatic data processing (ADP) systems under his or her cognizance. Only MAJCOM SIOs may appoint CSSOs to ensure executive-level support within each contracting firm.

(2) Ensure proper protection, dissemination, and use of SCI documents and material by enforcing all SCI information, personnel, physical, communications, TEMPEST, and ADP security rules and by developing good security policies and practices.

(3) Maintain the integrity of the SCI control system and ensure that personnel assigned to the SSO do not perform duties or details that conflict or interfere with their SCI security responsibilities or with the security of SCI. Collateral security management and foreign disclosure functions may not be assigned to full-time SCI security officials.

(4) Review and validate the need-to-know for SCI billets, the need for SCIFs, and the requirement for SCI communications and ADP systems. Approves selected SCI billets, redesignations, and realignments.

(5) Establish a Memorandum of Agreement (MOA) with the supporting Air Force Communications Command (AFCC) element to ensure SCI security, timely communications support to the intelligence mission, and privacy communications support.

(6) Identify communications-electronics (C-E) and communications security (COMSEC) needs to the supporting AFCC element commander.

(7) Ensure the SSO is functionally subordinate to and works directly for the SIO (the SIO should write the officer effectiveness reports (OER)).

(8) Establish training programs for SCI security officials. The scope of training provided must ensure the SCI security official can adequately perform the duties and requirements in USAFINTEL 201-1.

(9) Ensure sufficient qualified personnel, funds, and logistical support are provided to effectively operate the SSO system and the SCI security program, and to inspect field activities.

(10) Ensure appropriately SCI-cleared and -designated individuals within the organization understand existing regulations and guidelines governing the decompartmentation and sanitization of SCI (peacetime and emergency use) and establish continuing education and training programs for these personnel.

(11) Ensure that all commanders comply with responsibilities in e below and that all behavior data that pertains to SCI-indoctrinated individuals is reported expeditiously to HQ

USAF/INS as required by USAFINTEL 201-1.

(12) Keep the SSO informed of any issue that surfaces at the base Facilities Utilization Board (FUB), Communications-Computer Systems Requirements Board (CSRB), Base Security Council, and similar forums which might have SCI implications.

d. 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 SCIFs. Each SSO is directly responsible to the SIO, and must:

(1) Supervise the operation of the SSO and administer the SCI security program. Conduct or manage required SCI information, personnel, communications, TEMPEST, and physical security actions and procedures according to USAFINTEL 201-1 guidance.

(2) Ensure SCI is properly used, stored, accounted for, controlled, safeguarded, packaged, transmitted, and destroyed.

(3) Provide advice and assistance on SCI classification, control systems, sanitization, downgrading, decompartmentation, operational use, and emergency use.

(4) Ensure SCI is sent only to persons authorized access to the material and who have a verified need-to-know.

(5) Ensure all individual positions which require SCI access are "S" coded by manpower in the unit manning document (UMD) in the Automated Personnel Data System (APDS) according to AFR 300-4, volume I.

(6) Retain SCI security cognizance of the DSSCS Telecommunications Center (TCC) or Consolidated Telecommunications Center (CTCC), and interface with the TCC and ADP facilities to ensure proper SCI security and service to the SIO.

(7) Conduct SCI security briefings, indoctrinations, debriefings; obtain signed nondisclosure agreements and perform other related personnel security actions.

(8) Inspect all subordinate SCIFs annually, documenting the inspection results, and recommend corrective action and follow-up on corrective measures.

(9) Investigate SCI security infractions occurring in areas under the SSO's SCI security cognizance, make recommendations, and prepare required reports. Coordinate with host base and MAJCOM information security program managers (ISPM), as appropriate.

(10) Provide privacy communications support to flag rank officers residing on or transiting the base, and to other senior officers or offices as requested.

(11) Develop and conduct a continuing SCI Security Education, Awareness, and Training Program. Coordinate with host base and MAJCOM ISPM, as appropriate.

(12) Perform SCISO functions for the SSO office and oversee the performance of SCISOs for each subordinate SCIF.

e. All Commanders and Supervisors. All commanders and supervisors (who have SCI-indoctrinated individuals within their units or organizations) must forward all derogatory information received regarding any SCI-indoctrinated individual expeditiously to the SSO who will prepare a Behavior Data Report according to USAFINTEL 201-1. This includes any arrests, disciplinary actions, letters of counseling or reprimand, Article 15 actions, incidents involving alcohol or drug abuse, etc. See paragraph 4c.

f. Director, Base Medical Service. The medical community provides the commander important information about a person's continued eligibility for SCI access and information about treatment which may temporarily affect an SCI-cleared individual's ability to perform sensitive duties. The specific responsibilities of the director, base medical service, are detailed in AFR 35-36.

g. Chief, Security Police. The chief, security police provides security support for approved SCI facilities, and according to AFRs 125-37, DOD 5200.1-R/205-1, 205-32, and 207-1 and USAFINTEL 201-1:

(1) Ensures procedures are established to enable security teams to respond to SCIF alarms in a timely manner.

(2) Allows the unit commander, SSO, or designated representative to have access to daily blotter inputs bearing on the conduct of SCI-cleared personnel which may affect their continued SCI access.

(3) Establishes the SCI facility as a controlled area as specified in AFR 125-37 or, if justified by mission, establishes a restricted area according to AFR 207-1 and protects the area according to AFR 207-5.

h. Base TEMPEST Officer and Noncommissioned Officer (NCO). While the ACS/I through HQ USAF/INS is the TEMPEST authority for SCIFs, base TEMPEST officers and NCOs have certain responsibilities. These include ensuring that equipment and systems are installed accord-

ing to TEMPEST criteria and for conducting annual Red/Black inspections. Base TEMPEST officer and NCO responsibilities are contained in AFR 56-16, Control of Compromising Emanations (TEMPEST), and USAFINTEL 201-1.

i. Base Civil Engineer (BCE). The BCE must:

(1) Ensure all facilities to be designated as SCIFs are constructed or modified according to the standards outlined in DIAM 50-3, Physical Security Standards for Sensitive Compartmented Information Facilities, unless waived by HQ USAF/INSC.

(2) Ensure any requests for SCI-level shielded enclosures are accompanied by a National COMSEC Instruction (NACSI) 5004 or NACSI 5005 analysis, accomplished with the coordination of the host base or MAJCOM TEMPEST official, and a letter or message from HQ USAF/INSC stating the shielded enclosure is necessary for the proposed SCIF.

(3) Ensure requests for assistance on security-related problems in SCIFs are handled on a priority basis.

j. Air Force Communications Command (AFCC). Besides SIO and SSO responsibilities previously listed, AFCC must:

(1) Operate and maintain dedicated intelligence communications systems and CTCCs to provide timely intelligence communications support.

(2) Provide C-E and COMSEC programming for communications according to the supported unit's validated requirements, and maintain the Communications Electronic Authorization Program (CAP) for TCCs.

(3) Ensure TCC personnel are continuously trained and qualified in all aspects of DSSCS operating procedures.

(4) Implement approved communications plans and programs.

(5) Appoint the COMSEC officer and COMSEC custodian from appropriately cleared personnel.

(6) Provide resources on a rapid response basis to meet the needs for communications service during peak activities, catastrophes, or fluctuations in the intelligence mission, according to priorities established in the circuit restoration priority list or other authoritative source, such as MAJCOM operations plan or local directive.

(7) Inspect and evaluate the communications services provided SIOs.

(8) Retain basic personnel security responsibility for SCI-indoctrinated AFCC personnel, with the exception of SCI indoctrinations and debriefings, clearance access certifications, and transfer-in-status actions which are normally performed by a supporting SSO.

k. Electronic Security Command (ESC). Besides SIO and SSO responsibilities previously listed, ESC must:

(1) Maintain an ERAFSSO capability to fulfill the emergency and contingency operational requirements of MAJCOMs and Air Force-supported unified and specified commands.

(2) Manage selected CRITICOMM terminals. (AFCC maintains and operates these terminals.)

1. Unified and Specified Commands. When supported or staffed by Air Force elements (less air component commands of the unified commands), these commands establish and operate SSOs and other SCIFs according to DIA policies and rules. They advise the ACS/I and HQ USAF/INS of matters that impact on Air Force resources or SCI security. Air component commands of the unified commands will follow USAFINTEL 201-1. SCI access eligibility policy and rules for Air Force personnel assigned to the unified and specified commands will be according to USAFINTEL 201-1, chapter 3.

4. Personnel Security:

a. Investigation. A Special Background Investigation (SBI) or SBI-Periodic Reinvestigation (SBI-PR) is a prerequisite and must be conducted on all persons being considered for or having access to SCI. The SBI and SBI-PR collect information on a person's background and lifestyle to determine stability, character, and loyalty.

(1) An SBI completed according to DOD 5200.2-R/AFR 205-32 meets the investigative requirements for SCI access. The SBI consists of local agency checks, a National Agency Check (NAC), credit checks, neighborhood checks, education checks, and interviews of employment and developed references. It also includes a NAC on the individual's spouse and immediate family of 18 years or over who are United States citizens other than by birth or who are resident aliens.

(2) An SBI-PR completed according to DOD 5200.2-R/AFR 205-32 meets the intended scope of reinvestigative requirements of SCI access. The SBI-PR consists of investigative

actions for the previous 5 years. SBI-PRs are initiated for personnel currently SCI indoctrinated or personnel with less than a 1-year break in SCI access. SBI-PRs are conducted on a 5-year recurring basis for all persons authorized SCI access.

(3) Supervisors are now required to review DD Form 398, Personnel Security Questionnaire (BI/SBI), to ensure that no significant adverse information of which they are aware and which may have a bearing on an individual's continued eligibility for access to classified information is omitted. Supervisors will sign and date a statement to this effect in the remarks block of the DD Form 398.

(4) The results of the SBI and SBI-PR are sent by the Defense Investigative Service (DIS) to the Air Force Security Clearance Office (AFSCO) for adjudication for access to Top Secret information. If an individual is determined eligible for access to Top Secret information and has a requirement for SCI access, the investigative results are sent to HQ USAF/INSB for SCI adjudication.

b. Adjudication. SCI adjudication is the examination of data collected on an individual's lifestyle and behavior to ascertain whether the individual is eligible for SCI access. The key factors considered are the individual's maturity and sense of responsibility, to include trustworthiness, loyalty, and discretion. Adjudicators evaluate all pertinent information available against the established personnel security standards contained in DCID 1/14 and USAFINTEL 201-1, chapter 3, and adjudication guidelines. Any doubt concerning the individual's eligibility is always resolved in favor of national security. Commanders must screen, select, and nominate only those individuals who are stable, trustworthy, reliable, of excellent character, judgment, and discretion; and of unquestionable loyalty to the United States and who will remain in the position requiring access to SCI for at least 1 year.

c. Behavior Data Reporting. The Behavioral Data Reporting (BDR) system provides the MAJCOM SSO and SIO and HQ USAF/INS with timely information on personal status changes and incidents of personal behavior which might affect continued SCI eligibility. This system requires commanders and supervisors to report to their SSOs any changes and incidents ivolving SCI-indoctrinated persons (military, Air Force civilians, contractors, and consultants) as well as the person's immediate family (when SCI access eligibility is, or might be affected). The SSO ensures formal BDR according to USAFINTEL 201-1, chapter 3. (This is not a reporting requirement of the medical service.)

d. Due Process Procedures for SCI Access Denials. HQ USAF/INS notifies each individual through his or her commander when SCI access has been denied or revoked. 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 acknowledgement to file an appeal. If the appeal is denied, the individual has 30 calendar days from the date of the appeal letter to request his or her SCI access disapproval be reviewed by ACS/I. The ACS/I's determination is final and unreviewable.

e. "For Cause" Actions—Persons Being Considered for Court-Martial, Involuntary Separation, Discharge, or Dismissal. When an SCI-indoctrinated individual is being considered for involuntary separation from the Air Force, dismissal from civilian employment with the Air Force, or court-martial (general or special), no action will be taken until the proposed action has been reviewed and approved by HQ USAF/INS. Processing procedures for "For Cause" cases are contained in DOD 5200.2-R/AFR 205-32 and USAFINTEL 201-1, chapter 3.

5. SCI Billets. An SCI billet is a position in which the incumbent requires knowledge and access to SCI to perform his or her official duties. SCI billets are used throughout the Department of Defense to record these positions and are authorized only after verification of need-to-know. HQ USAF/INS approves or obtains approval from other authorities for billets for all organizations under the ACS/I SCI security cognizance. The MAJCOM SIOs have the authority to approve selected billets, realignments, and redesignations for organizations under their cognizance as specified in USAFINTEL 201-1, chapter 2.

a. Criteria for Justifying SCI Billets. On determining that a need-to-know exists, submit a billet request using sufficient justification which spells out the need-to-know.

b. Requesting an SCI Billet. When preparing

billet request packages, use the actual duty title, not the Air Force Specialty Code (AFSC) nor the UMD title, unless the AFSC or UMD fully describes the position. USAFINTEL 201-1, chapter 2, provides specific guidelines for submitting a billet request for military and civilian billets, contractor performance and service billets, consultant billets, Air Force Reserve billets, base support billets, student billets, and special purpose access (SPA).

6. Indoctrinations and Debriefings. USAFINTEL 201-1, chapter 4, requires that all personnel approved for access to SCI receive a basic, yet comprehensive, indoctrination on the sensitivity of SCI, and its security, use, and dissemination. The directive also requires reindoctrination every 2 years, as well as a formal debriefing when SCI access is terminated. HQ USAF/INSC provides standard Air Force SCI indoctrination and debriefing materials (including video tapes and hard copy briefing packages) to field SSOs. SSOs:

a. Conduct indoctrinations using this material.

b. Supplement the indoctrinations with all local security procedures.

c. Conduct formal reindoctrinations of SCI-indoctrinated individuals at 2-year intervals.

d. Conduct SCI debriefings whenever an individual no longer has a need-to-know or when directed by HQ USAF/INS.

e. Supplement these formal indoctrinations and debriefings with continuing SCI awareness training to all SCI-indoctrinated individuals under their cognizance (see paragraph 12).

7. Access to SCI:

a. Control of Access. Access to SCI must be kept to the absolute minimum consistent with HQ USAF approved SCI eligibility, valid need-to-know, and the operational mission. Besides the required SBI and adjudication by HQ USAF/INS, all persons who need access to SCI must be nominated to and approved by HQ USAF/INS who will then authorize their indoctrination. Simply having an up-to-date SBI adjudicated by HQ USAF/INS is never authority to have access to SCI. Once indoctrinated for SCI, access to SCIFs is not automatic. SCI-indoctrinated persons desiring to visit other SCIFs on SCI business must have their SCI accesses certified through SSO channels. Visits by contractors and consultants with SCI access must be carefully reviewed to ensure the visit is on contractual business and that their SCI accesses have been certified.

b. Two-Person Rule. The DCI has established a stringent policy on the staffing of SCIFs. As a matter of policy, SCIFs must be staffed with sufficient people to deter unauthorized copying or illegal removal of SCI. SCIFs must be staffed at all times by at least two appropriately indoctrinated persons in proximity to one another to provide mutual support in maintaining the integrity of the facility and the material stored there. Access to or work by a lone individual in an SCI facility is not allowed.

c. Special Purpose Access (SPA). SPA is used for personnel who require SCI access for short durations (not to exceed 90 days) or who are in positions which would not warrant an SCI billet. The request, which includes detailed justification, is sent to HQ USAF/INSB. The unit SIO must concur with the request. The MAJCOM SIO and the unit SIO must ensure SPAs are managed within authorized guidelines. No further action is required by the MAJCOM unless they nonconcur with the request.

d. Emergency SCI Access. Emergency SCI access is used for personnel who require SCI access before meeting the eligibility standards set forth in DCID 1/14 and USAFINTEL 201-1. The person must be on station and there must be an urgent requirement to have the individual indoctrinated into an approved billet. The request, which includes detailed justification, is sent to HQ USAF/INSB. The local SIO and MAJCOM SIO must certify that the emergency exists and that the person must have immediate SCI access.

8. Physical Security. Any Air Force commander may request a SCIF if there is a validated need to process, use, discuss, or store SCI and the desired facility meets the minimum physical security standards outlined in DIAM 50-3. There are three basic steps for getting a facility accredited as a SCIF. The requestor must submit the following packages to the local SSO for further processing. (Specific information and detailed guidance are contained in USAFINTEL 201-1, chapter 5.)

a. Concept Validation Request. This is the first step to establishing a SCIF and is a key element in future accreditation actions. In this letter, the requester describes why the SCIF is needed (program being supported), the location and accreditation level desired, agencies and organizations to be serviced by the SCIF, type

of work to be done in the facility, and proposed operational hours. The requester also includes a statement of certification that there is currently no other SCIF in the area which could satisfy the requirement.

b. Preconstruction Review Package. In this next step, the requester prepares a preconstruction checklist (DIAM 50-3, enclosure 5), which describes planned construction, access control devices, alarm systems, guard personnel, etc. Careful planning is essential when preparing this package, as it describes how the construction and physical security standards will be met.

c. Accreditation Package. This is the last step in the accreditation process. The requester prepares another checklist (DIAM 50-3, enclosure 5), which describes how the facility was actually constructed and what physical security measures were implemented. SCI may not be discussed or introduced into a proposed SCIF until HQ USAF/INSC approves this package and accredits the facility as a SCIF.

d. Physical Security Support. The SCIF must be protected as a controlled area or as an Air Force priority resource depending on mission. Before accreditation is complete, the base security council should review mission and address physical protection. A copy of the security council recommendations should be a matter of record in the accreditation package.

e. Exceptions. The above procedures apply to fixed, permanent, non-ESC SCIFs only. For mobile SCIFs, temporary secure working areas, or ESC SCIFs, contact the local SSO or review USAFINTEL 201-1, chapter 5.

9. SSO Staffing. Due to the complexity of SCI security management responsibilities and the requirements of the two-person rule for SCIFs, minimum staffing for each SSO is three personnel. Local SIOs should justify requests for exceptions or waivers to this policy in writing to HQ USAF/INSC, through the MAJCOM SIOs who will add their recommendations.

10. COMSEC and Computer Security (COMPUSEC):

a. Each piece of telecommunications, ADP, electrical, and electromechanical equipment which will be used to process SCI, or which will be used to process unclassified or collateral classified information in a SCIF, must be accredited to HQ USAF/INSC for use at the required specific level before commencing operations. TEMPEST accreditation is obtained by submitting required checklists according to USAFINTEL 201-1, chapter 6.

b. ADP systems using software require two separate accreditations or approvals: a TEMPEST accreditation (as described above) and a software system accreditation. ADP system accreditation for SCI operations must be submitted according to USAFINTEL 201-1, chapter 8. (ADP system accreditations for collateral use must be submitted according to AFR 205-16.) No processing is authorized until the system has received both the ADP systems accreditation and the TEMPEST accreditation.

11. SCI Security Incidents and Violations. Incidents involving possible compromise or improper handling of SCI material must be reported immediately as directed in USAFINTEL 201-1, chapter 18. An SCI security incident is any event that actually or potentially jeopardizes the security of SCI or could lead to a compromise, deviation, or practice dangerous to security. Any incident of this nature must be reported immediately to the closest SSO. Security police personnel, unless they are an SSO, are not authorized to investigate SCI security violations.

a. The SSO will report, initiate, and ensure inquiries or investigations are conducted on all SCI security incidents, except those referred to the Air Force Office of Special Investigation (AFOSI) or the Federal Bureau of Investigation (FBI). The SSO will remain the office of primary responsibility until the case is formally closed. SSOs will ensure all reports are prepared and act as the focal point for other investigative agencies involved in the SCI security incident. Contractor SSOs will report and investigate SCI security incidents in the same way as Air Force SSOs.

b. Besides the obvious security violations that must be reported, USAFINTEL 201-1 also requires that incidents involving SCI-indoctrinated military members, contractors or DOD civilians who either fail to report to duty or return from an assigned mission and whose whereabouts cannot be positively determined, be treated as security violations. Also, any act which could lead to compromise or a security violation if corrective action is not taken must be reported. For example, an SCI courier who stops at a public shopping area must be reported as a security violation.

c. Unlike security violations reported under

DOD 5200.1-R/AFR 205-1, 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 HQ USAF/INS or DIA.

12. Security Education, Awareness, and Training. The SCI Security Education, Awareness, and Training Program is designed to increase the security awareness of US Air Force military, civilian, and contractor personnel working under the SCI security cognizance of the ACS/I. The program runs from initial SCI indoctrination through debriefing, with continuing education, awareness, and training in between. The program implements DCID 1/14, annex C, and USAFINTEL 201-1, chapter 19. HQ USAF/INSC manages and evaluates the SCI Security Education, Awareness, and Training Program to include producing and distributing indoctrination and debriefing materials, continuing and special education and training materials, security advisories, policy related guidance, and conducting appropriate training courses. Each SSO must manage, conduct, and evaluate local and subordinate SCI security education and training to include all indoctrinations, reindoctrinations, debriefings, and periodic SCI awareness training.

BY ORDER OF THE SECRETARY OF THE AIR FORCE

OFFICIAL

LARRY D. WELCH, General, USAF
Chief of Staff

NORMAND G. LEZY, Colonel, USAF
Director of Information Management
and Administration

SUMMARY OF CHANGES

This revision clarifies management of the SCI security system within the Air Force and details the responsibilities of the ACS/I, SIOs, SSOs, SCISOs, and commanders and supervisors of SCI-cleared personnel (para 3); sections are included for security police commanders, medical facility commanders, civil engineering commanders, communications commanders, and TEMPEST officers and NCOs (para 3); specific sections are added on personnel security (para 4), SCI billets (para 5), indoctrinations and debriefings (para 6), access to SCI (para 7), physical security (para 8), SSO staffing (para 9), COMSEC and COMPUSEC (para 10), SCI security incidents and violations (para 11), and SCI education, awareness, and training (para 12).

GLOSSARY OF ABBREVIATIONS

ACS/I	Assistant Chief of Staff/ Intelligence
ADP	Automatic Data Processing
AF/INS	Air Force Directorate of Security and Communications Management
AFOSP	Air Force Office of Security Police
AFSCO	Air Force Security Clearance Office
ARFCOS	Armed Forces Courier Service
AUTOSEVOCOM	Automatic Secure Voice Communications
BI	Background Information
BDR	Behavior Data Report (or Reporting)
CIA	Central Intelligence Agency
COMPUSEC	Computer Security
COMSEC	Communications Security
CRITICOMM	Critical Intelligence Communications System
CSSO	Contractor Special Security Officer
DCI	Director of Central Intelligence
DCID	Director of Central Intelligence Directive
DIA	Defense Intelligence Agency
DIS	Defense Investigative Service
DOD	Department of Defense
DSSCS	Defense Special Security Communications System
DUSD(P)	Deputy Under Secretary of Defense (Policy)
EO	Executive Order
ERAFSSO	Emergency Reaction Air Force Special Security Office
ESC	Electronic Security Command
IC	Intelligence Community
ISPM	Information Security Program Manager
NAC	National Agency Check
NACSI	National COMSEC Instruction
NACSIM	National COMSEC Information Memorandum
NFIB	National Foreign Intelligence Board
NSA	National Security Agency
OPSEC	Operations Security
OSD	Office of the Secretary of Defense
OS	Office of Security, DIA
OSI	Office of Special Investigations
PR	Periodic Reinvestigation
SBI	Special Background Investigation
SCI	Sensitive Compartmented Information
SCIF	Sensitive Compartmented Information Facility
SCISO	Sensitive Compartmented Information Security Officer
SIO	Senior Intelligence Officer
SOIC	Senior Official of the Intelligence Community
SPA	Special Purpose Access
SPINTCOMM	Special Intelligence Communications
SSO	Special Security Office, Special Security Officer
USAFINTEL	United States Air Force Intelligence

☆U.S. G.P.O. 1987-180-958:70039