Director of Central Intelligence

SECURITY POLICY MANUAL FOR SCI CONTROL SYSTEMS (U)

Prepared for
The Director of
Central Intelligence
by the
Security Committee

Confidential

28 June 1982

Warning Notice
Intelligence Sources and Methods Involved
(WNINTEL)

NATIONAL SECURITY INFORMATION
Unauthorized Disclosure Subject to Criminal Sanctions

DISSEMINATION CONTROL ABBREVIATIONS

NOFORN–	Not Releasable to Foreign Nationals
REL . . .–	This Information has been Authorized for Release to . . .
NOCONTRACT–	Not Releasable to Contractors or Contractor/Consultants
PROPIN–	Caution—Proprietary Information Involved
ORCON–	Dissemination and Extraction of Information Controlled by Originator

25X1

Approved For Release 2005/12/14 : CIA-RDP87B01034R000500180008-4

DIRECTOR OF CENTRAL INTELLIGENCE

SECURITY POLICY MANUAL FOR SCI CONTROL SYSTEMS (U)

(Attachment to "Security Policy for Sensitive Compartmented Information (SCI)"

TABLE OF CONTENTS

SECURITY POLICY MANUAL FOR SCI CONTROL SYSTEMS

Introduction

This manual contains security policy and procedures common to the several SCI control systems for the protection of intelligence information. Users should refer to DCIDs and other documents referenced herein for specific guidance on the functional areas they cover. Users are also reminded that they should refer to the applicable SCI control system manuals or directives for guidance on what information is to be classified at what level and protected by compartmentation.

Questions on this manual should be directed to the DCI Security Committee (SECOM) if not answerable by security components of Intelligence Community organizations.

As this manual sets forth security policy and procedures for SCI control systems, it merits and warrants the overall classification of CONFIDENTIAL in its totality. Selected paragraphs may be excerpted for use at the unclassified (Official Use Only) level by Senior Officials of the Intelligence Community (SOICs), their designees, or SCI Special Security/Control Officers, when considered appropriate.

1. Definitions

a. ***Document***—any recorded information regardless of its physical form or characteristics, including, without limitation, written or printed matter, automated data-processing storage media, maps, charts, paintings, drawings, photos, engravings, sketches, working notes and papers, reproductions of such things by any means or process, and sound, voice, magnetic, or electronic recordings in any form.

b. ***Hardcopy Document***—any document that is initially published and distributed by the originating component in paper form and that is not stored or transmitted by electrical means.

c. ***Intelligence Community***—those United States Government organizations and activities identified in Executive Order 12333 or successor orders as making up such Community.

d. ***Raw Intelligence***—collected intelligence information which has not yet been converted into finished intelligence.

e. ***Sensitive Compartmented Information (SCI)***—all information and materials requiring special Community controls indicating restricted handling within present and future Community intelligence collection programs and their end products. These special Community controls are formal systems of restricted access established to protect the sensitive aspects of sources and methods and analytical procedures of foreign intelligence programs. The term does not include Restricted Data as defined in Section II, Public Law 585, Atomic Energy Act of 1954, as amended.

f. ***SCI Facility (SCIF)***—an accredited area, room, group of rooms, or installation where SCI may be stored, used, discussed and/or electronically processed.

g. ***Senior Officials of the Intelligence Community (SOICs)***—for the purposes of this manual, SOICs are defined as the heads of organizations within the Intelligence Community, as defined by Executive Order 12333, or their designated representatives.

PERSONNEL SECURITY

2. **General.** The protection of SCI is directly related to the thoroughness and effectiveness of the personnel security program applicable to those individuals having access to such information. An interlocking and mutually supporting series of program elements (e.g., need-to-know, investigation and adjudication in accordance with DCID 1/14, "Minimum Personnel Security Standards and Procedures Governing Eligibility for Access to SCI," binding contractual obligations on those granted access, security orientation, and continuing security oversight) can provide reasonable assurances against compromise of SCI by those authorized access to it.

3. **Need-to-Know Policy.** The first personnel security principle in safeguarding SCI is to ensure that only those persons with a clearly identified need-to-know are granted access to it. Need-to-know is a determination by an authorized holder of classified information that access to specific classified material in his or her possession is required by one or more other persons to perform a specific and officially authorized function essential to accomplish a national security task or as required by Federal Statute, Executive Order, or directly applicable regulation.

4. **Standards.** Personnel security standards, reporting of data bearing on SCI eligibility, investigative requirements, reinvestigations, adjudications, and supervisory security responsibilities shall be in accordance with DCID 1/14.

5. **SCI Nondisclosure Agreements (NdAs).**

a. All persons holding or being given SCI access shall sign an NdA. Failure to sign an NdA is cause to deny or revoke existing SCI access to the refusing person. The NdA establishes explicit obligations on both the Government and the individual signer in the interest of protecting SCI. Form 4193, "Sensitive Compartmented Information Nondisclosure Agreement," is available for use. It includes a prepublication review provision. Use of a prepublication review provision in any alternative form of NdA is mandatory. Any department or agency electing to use an alternative form of NdA shall use it without exception for all SCI accesses.

b. Further information on Form 4193 may be found in the July 1981 "Questions and Answers for Use with the Sensitive Compartmented Information Nondisclosure Agreement" prepared for use by government and industry security officers.

6. **Recording Indoctrinations and Debriefings.** Briefing officers shall appropriately record certifications of all SCI indoctrinations and debriefings they accomplish. Administrative guidance on NdAs, indoctrination and debriefing forms, and related procedures shall be specified by SOICs for areas under their cognizance.

7. **Access Approvals.** When need-to-know has been established and investigative results have been satisfactorily adjudicated, SCI accesses shall be granted and formally recorded.

a. ***Authority.*** SCI accesses shall be granted by the SOIC having cognizance of the persons involved. For persons in non-NFIB government organizations, SCI accesses are granted by the DCI through the CIA Special Security Center (SSC). Unless specifically delegated, approval authority for access to certain operational collection systems is retained

by the cognizant program manager, executive agent or national authority. Administrative procedures governing the granting of SCI accesses shall be specified by SOICs for their organizations.

b. *General SCI Approvals*—"PROXIMITY." A "PROXIMITY" approval may be granted by, and at the discretion of, the cognizant SOIC to persons who closely support SCI collection, processing, or use but whose duties do not warrant granting substantive SCI access approvals. PROXIMITY allows the holder to perform his or her duties in support of any SCI control system provided the tasks do not involve visual or aural access to clear text, intelligible SCI.

(1) PROXIMITY approvals may also be granted, according to the criteria in (2) below, when a person is authorized one or more SCI access approvals. For example, substantive access to COMINT may be required when PROXIMITY will suffice for another SCI access.

(2) Minimum criteria for PROXIMITY approval areas follow:

(a) The nature of the individual's support to SCI involves a substantial latent risk of exposure to SCI through inadvertence or a deliberate effort by the individual.

(b) Approval for a specific SCI System or project would provide the person more information than needed, either in the indoctrination or by virtue of the access approval, or both.

(c) The individual does not need to know substantive SCI in order to perform his or her function and shall not receive access in the normal course of his or her duties.

(d) The individual's potential for access is such that personnel security assurances provided through investigations and adjudication for collateral clearances are not deemed adequate by the cognizant SOIC or designee.

(3) Persons determined by their SOIC to require PROXIMITY approval shall be processed to DCID 1/14 personnel security standards. They shall be given a non-SCI revealing briefing notifying them that their duties may bring them in close proximity to highly sensitive government information; cautioning them to report to their security officer any inadvertent access involving them; and providing them a generalized description of the appearance of SCI documents (e.g., material may have color-coded cover sheets, and shall bear handling system caveats) to enable them to recognize such material if it is exposed to them.

(4) NdAs are required of persons being granted PROXIMITY approval to obligate them to observe the agreement's provisions with respect to any SCI of which they might gain knowledge. If an inadvertent disclosure is made to a person with PROXIMITY approval, that person shall be given a security briefing to ensure that he or she understands the applicability of the NdA and his or her obligations under it.

(5) SOICs shall administer PROXIMITY approvals for those persons they sponsor. Once granted, the PROXIMITY approval is valid within the cognizance of the granting SOIC.

(6) To the extent that SOICs find it practicable, individuals already holding substantive access approvals may be converted to PROXIMITY if they meet the tests

for such. Those so converted shall be cautioned not to discuss with other PROXIMITY approved persons their previously acquired knowledge of SCI. SOICs are expected to exercise prudence in extending PROXIMITY approvals to persons and positions not now requiring SCI access approvals in order to avoid undue burden on the SCI personnel security system. Substantive access approval requests shall normally take precedence over PROXIMITY requests.

8. **Central Registry.** A Community-Wide, Computer Assisted, Compartmentation Control System (4C system) is being established by the DCI. Each SOIC granting or terminating SCI accesses and PROXIMITY approvals shall record such actions in the 4C system. SOICs are responsible for establishing procedures for the certification of SCI accesses to other components.

9. **Security Indoctrination and Education.**

a. Prior to signing the NdA or being afforded access to SCI, persons approved for SCI access shall be given a non-SCI revealing briefing on the general nature and procedures for protecting the SCI to which they will be exposed, advised of their obligations both to protect that information and to report matters of security concern, and allowed to express any reservations concerning the NdA or access to SCI.

b. Subsequent to signing the NdA, persons shall be fully indoctrinated on the aspects of the SCI to which they are authorized access and have a demonstrated need-to-know. All persons granted SCI access shall periodically be advised of their continuing security responsibilities and of security threats they may encounter. DCI SECOM-D-543, July 1979, "Minimum Standards for Security Awareness Programs in the U.S. Intelligence Community," provides guidance.

10. **Foreign Contacts.** Close, continuing personal associations with foreign nationals by persons with SCI access are of security concern. Persons with SCI access shall be informed of their continuing responsibility to report all non-official contacts with representatives or citizens of Communist-controlled countries and of other countries which are hostile to the United States. SOICs shall ensure that their SCI-indoctrinated personnel are kept informed of which countries are of concern in this regard. SCI-indoctrinated persons are also responsible for reporting contacts with persons from other than Communist-controlled or hostile countries whenever those persons show undue or persistent interest in employment, assignment, or sensitive national security matters. Contacts, or failure to report contacts, in either of the above situations shall result in reevaluation of eligibility for continued SCI access by the cognizant SOIC. Casual contacts arising from living in a community and which do not fall within either of the above situations normally need not be reported.

11. **SCI Travel and Assignment Security Policy.** Persons with current SCI access who plan unofficial travel to, or who are being assigned to duty in, foreign countries and areas, particularly those identified in DCID 1/20, "Security Policy Concerning Travel and Assignment of Personnel With Access To SCI," incur a special security obligation. This includes requirements to provide advance notice of unofficial travel and to be afforded appropriate defensive security briefings prior to official assignment or unofficial travel. Minimum security policy applicable to such travel or assignment is stated in DCID 1/20.

PHYSICAL SECURITY

12. **Construction and Protection Standards.** All SCI must be stored within accredited SCIFs. Physical security standards for the construction and protection of such facilities are

prescribed in NFIB/NFIC-9.1/47, "U.S. Intelligence Community Physical Security Standards for SCI Facilities," effective 23 April 1981, or successor policy statements.

13. **Accreditation of SCIFs.** The DCI shall accredit all SCIFs except where that authority has been specifically delegated or otherwise provided for. The CIA Office of Security shall accredit SCIFs for Executive Branch departments and agencies outside the Intelligence Community and for the Legislative and Judicial Branches. The accreditation shall state the category(ies) of SCI authorized to be stored/processed in the SCIF. Accrediting officials shall maintain a physical security profile on each of their SCIFs to include data on any waivers of standards.

14. **Emergency Plans.** Each accredited SCIF shall establish and maintain an approved emergency plan. This may be part of an overall department, agency, or installation plan, so long as it satisfactorily addresses the considerations stated below. Emergency planning shall also take account of fire, natural disasters, entrance of emergency personnel (e.g., host country police and firemen) into a SCIF, and the physical protection of those working in such SCIFs. Planning should address the adequacy of protection and firefighting equipment, of evacuation plans for persons and SCI, and of life-support equipment (e.g., oxygen and masks) that might be required for personnel trapped in vault-type SCIFs.

a. In areas where political instability, host country attitude, or criminal activity suggests the possibility that a SCIF might be overrun by outsiders, emergency plans must provide for the secure destruction/removal of SCI under adverse circumstances, to include such eventualities as loss of electrical power, nonavailability of open spaces for burning or chemical decomposition of material, and immediate action to be taken if faced with mob attack. Where the risk of overrun is significant, holdings of SCI must be reduced to, and kept at, an absolute minimum needed for current working purposes, with reference or background material to be obtained, when needed, from other activities and to be returned or destroyed when it has served its purpose.

b. Emergency plans shall be reviewed annually and updated as necessary. All personnel shall be familiar with the plans. In areas where political or criminal activity suggests the possibility that the SCIF might be overrun by outsiders, drills shall be conducted as local circumstances warrant but no less frequently than annually to ensure testing and adequacy of plans.

15. **Two-Person Rule.** NFIB/NFIC-9.1/47 establishes policy on this subject, which is quoted below for ready reference:

> "As a matter of policy, SCI Control Facilities (SCIFs) should be staffed with sufficient people to deter unauthorized copying or illegal removal of SCI. SCIF designated communication centers, document control centers (registries), and like facilities that handle or store quantities of SCI must be manned while in operation by at least two appropriately indoctrinated persons in such proximity to one another as to provide mutual support in maintaining the integrity of the facility and the material stored therein. The granting by an SOIC of exceptions to this policy will be made a matter of record and should involve consideration of the proven reliability and maturity of the persons involved; the volume, variety, and sensitivity of the holdings in the facility; and whether or not the persons involved are subject to periodic polygraph examinations as a condition of access. Exceptions for communications centers, document control centers, and the like should be granted in only extraordinary

circumstances. Routine work by a lone individual in any SCIF is to be avoided. Contractors will provide two-person occupancy in all SCIFs not specifically exempted by the SOIC of the government sponsor."

When a SCIF is granted a waiver for long-term occupancy by a single person, the responsible official shall also establish procedures to ensure that periodic visual or oral checks are made to provide assurances on the well-being of the single occupant. Duress alarms and/or duress codes are considered valuable tools to assist in overcoming problems associated with long-term occupancy of a SCIF by a single person.

TECHNICAL SECURITY

16. **Technical Surveillance Countermeasures.** Responsible SOICs shall ensure that technical surveillance countermeasures are conducted at their SCIFs at appropriate intervals. Briefings on technical penetration threats shall be provided to personnel manning SCIFs.

17. **Compromising Emanations Control Security (TEMPEST).** All equipment used to transmit, handle, or process SCI electronically, including communications, word-processing and automated data processing equipment, must satisfy the requirements of NCSC-4, "National Policy on Control of Compromising Emanations" and NACSIM 5203, "TEMPEST Guidelines for Facility Design and RED/BLACK Installations" (when published). Identified compromising emanations must be contained within appropriate boundaries. Instrumented TEMPEST tests shall be conducted at appropriate intervals to insure compliance with NCSC-4 or successor policy.

18. **Automated Data Processing (ADP) Security.** All ADP equipment used for processing, handling, or storing SCI shall be operated and secured in compliance with DCID 1/16, "Security of Foreign Intelligence in Automated Data Processing Systems and Networks," or successor policy directives.

SCI DOCUMENT CONTROL OFFICES/CENTERS AND SECURITY OFFICIALS

19. **SCI Special Security Offices and/or Control Centers.** SCI Special Security Offices and/or Control Centers, as appropriate, shall be established to serve as the focal point(s) for the receipt, control and accountability of SCI, and other SCI security functions for one or more SCIFs in the local area. The number of such offices and/or centers shall be determined locally on the basis of practicality, number of SCIFs to be serviced, organizations involved, and common sense.

20. **SCI Special Security/Control Officers.** Appropriately SCI-indoctrinated Special Security Officers and/or SCI Control Officers (e.g., SSOs, TCOs and/or BCOs), and alternates thereto, shall be designated to operate each SCI Special Security Office and/or Control Center. Such officials shall normally have day-to-day SCI security cognizance over their offices/centers and subordinate SCIFs, if any, for that SCI authorized to be handled by organizations served by them. Responsible SOICs shall provide appropriate training in SCI security policy and procedures for their SCI special security/control officers and other SCI registry/security personnel. SCI Special Security/Control Officers shall provide advice and assistance on SCI matters to their organizations and other activities being supported consistent with specific responsibilities assigned by their SOICs. This may include one or more of the following:

— ensuring that SCI is properly accounted for, controlled, transmitted, destroyed, packaged, and safeguarded;

— giving advice and guidance on SCI classification matters, sanitization, downgrading, decompartmentation, and operational use;

— ensuring that SCI is disseminated only to persons authorized access to the material involved and having an established need-to-know;

— conducting or otherwise managing required SCI personnel and physical security actions and procedures;

— investigating SCI security infractions and preparing reports and recommendations as required;

— maintaining listings of available SCI electrical and hardcopy products, validating product requirements, and ensuring dissemination to authorized users; and/or

— conducting required supervision or interface with SCI telecommunications centers, ADP facilities, and similar offices to ensure SCI security.

INFORMATION SECURITY

21. **Standard Classification Marking Requirements.** Apply standard security classification markings (to include classification authority and declassification markings) to SCI according to Executive Order 12356 or successor orders and Executive Branch implementing directives. SCI shall always bear the notation "ORIGINATING AGENCY'S DETERMINATION REQUIRED (OADR)" in lieu of any specific date or event for declassification.

22. **SCI Caveats, Codewords, and Designators.** Mark SCI with the applicable SCI control system caveat at the bottom of all pages of hardcopy documents, to include the front and back covers, if any. Mark other SCI documents as described elsewhere in this manual. If the material is to be controlled in only one SCI control system, use either of the following styles:

"HANDLE VIA *(name of SCI control system)* CHANNELS ONLY"
"HANDLE VIA *(name of SCI control system)* CONTROL CHANNELS"

If the material is to be controlled in two or more SCI control systems, use the following style:

"HANDLE VIA *(names of SCI control systems)* CONTROL CHANNELS JOINTLY"

Mark SCI codewords, or operational program designators protection immediately following the security classification on all pages containing requiring SCI protection.

23. **Dissemination Control Markings.** When applicable to their information content, mark SCI with the dissemination control markings in the manner prescribed by DCID 1/7, "Control of Dissemination of Intelligence Information."

24. **Portion Marking.** Each copy of an SCI document (excluding raw intelligence or working materials) that is transmitted outside the originating agency or department shall, by marking or other means, indicate: (1) which portions are classified, with the applicable classification level, and which portions are not classified; and (2) which portions require SCI codewords, caveats, program designators, or DCID 1/7 control markings.

a. Abbreviations for classifications (i.e., "TS," "S," and "C," in descending order; "U" to designate unclassified items), authorized digraph or other recognized abbreviations for codewords and product indicators, authorized abbreviations for SCI control system caveats and DCID 1/7 control marking short abbreviations shall be used to show the security protection requirements of portions.

b. Alternatively, such as in the case of documents all of whose portions are of the same level of classification and control, a paragraph or statement on the document may be used to indicate the security protection requirements of document portions. Unless the usefulness of the document would suffer thereby, titles of SCI documents shall be so worded as to avoid the need for compartmented control and to minimize or eliminate the need for classification.

c. SOICs may grant waivers of the portion marking requirements for contractor-generated SCI when deemed necessary to alleviate an extreme administrative and/or costly burden. Waivers shall not be considered for any permanently valuable records of the Government, or for any information transmitted outside the facility. Any information transmitted outside the facility where it may be used as a source document in the derivative classification of other information, must be portion marked before its transmittal. Further, any document upon which the waiver is exercised shall be marked as follows:

"WARNING—THIS DOCUMENT SHALL NOT BE USED
AS A SOURCE FOR DERIVATIVE CLASSIFICATION"

25. Letters or Memoranda of Transmittal.

a. ***Classified Transmittal Letters.*** Mark transmittal letters that contain classified information or SCI with the highest classification and all SCI codewords, caveats, or control markings in the letter itself or any of its enclosures, with a notation such as the following:

"REGRADE AS *(classification, caveat/codeword, etc)* WHEN SEPARATED FROM ENCLOSURE(S) AND UPON PHYSICAL REMOVAL OF INAPPROPRIATE SCI CAVEATS, CODEWORDS, AND CONTROL MARKINGS"

In such cases, holders of the letter of transmittal letter must physically remove the inappropriate markings when the letter of transmittal is separated from the enclosure(s).

b. ***Unclassified Transmittal Letters.*** If a transmittal letter is unclassified itself, but has one or more SCI enclosures, mark it with the highest classification of the enclosure(s) and a prominent notation such as the following:

"CONTAINS *(BYE/TK/SI)* INFORMATION—
UNCLASSIFIED WHEN APPENDED SCI DOCUMENTS ARE REMOVED"

In such cases, do not mark the letter of transmittal with the SCI codewords or caveats contained on the enclosure(s).

26. **SCI Control Numbers.** Originators shall assign a control number to any SCI documents intended for general distribution to other offices, agencies, or commands, when use of a number is considered a necessary adjunct to identification, control, or retrieval of the material. Blocks of control numbers will be assigned to SOICs by the CIA Compartmented Information Branch or other appropriate authority. Control numbers, at a minimum, shall be placed in the designated block on cover sheets and on the front cover (if any) and the title page (if any)—or, if no cover or title page, on the first page.

a. Each control number shall consist of the identifying letters of the name of the applicable control system, a number selected on a "one up" basis from the block of numbers assigned to the control office, and the last two digits of the current year. When a document contains SCI subject to two or more control systems, assign a control number according to the established precedence of SCI systems. For example, material containing BYE and TK or BYE and COMINT material would be assigned a BYE number. Material containing TK and

COMINT would be assigned a TCS number. SOICs may prescribe special numbering procedures for contractor-originated SCI.

b. When a control number is used, also assign a copy number to individual documents (e.g., copy 1 of 3 copies). Show the copy number with the control number. Use a combination of digits and letters to show reproduced copies (i.e., copy 1A, copy 4C, etc.) or identify the copies as "Series B," Series C," etc.

27. **Specialized Media.** Unless specifically excepted by the cognizant SOIC, labeling requirements for SCI in specialized media are as cited below.

a. ***Automated Data Processing (ADP) Media.*** Each media item [e.g., demountable data and program storage media (magnetic tapes, disk packs, floppy disks, magnetic cassettes), card decks, punched paper tapes] containing SCI in recorded form shall be externally labeled to show its classification and applicable SCI control system caveats or codewords. Internal ADP media identification shall include header and trailer blocks giving all security markings (i.e., classification; SCI system caveats, codewords, product indicators; and DCID 1/7 control markings, as applicable).

b. ***Photographic Media.*** Photography in roll, flat, or other form containing SCI shall be labeled with its classification and applicable SCI control system caveats or codewords. For film in roll form, a label giving the required data shall be placed on the end of the spool flange, on the side of the spool container, and on the container cover (if any), unless the container and its cover are transparent, in which case no label is needed on the container and or its cover if the flange label is visible through the container. Roll film itself shall include head and tail sequences giving all security markings applicable to the contents. Positive film flats or slides shall bear individual internal markings providing the classification and all applicable SCI and other control markings. The frames of slides shall also be labeled with the classification and applicable SCI caveats and codewords (which may be abbreviated if necessary to fit in the space provided).

c. ***Microform Media:***

(1) *Microfiche.* Each microfiche shall have a heading whose elements are readable without magnification and which provides the document title, classification, SCI control number, and, using standard abbreviations, applicable SCI caveats and codewords and DCID 1/7 control markings. Individual microfiche shall be placed in color-coded envelopes indicative of the SCI control system(s) applicable to the informational contents.

(2) *Microfilm.* Each roll of microfilm shall contain classification and control information at the beginning and end of the roll. This may be in abbreviated form. Boxes containing processed film on reels and film cartridges shall be labeled to show the document title (generic title if more than one document is on the film), the highest security classification of the contents, the SCI caveats and codewords applicable to the filmed information, and any DCID 1/7 control markings that may apply.

d. ***Electrically Transmitted Traffic.*** SCI transmitted by accredited electrical or electronic means resulting in record copy material shall be marked at the top and bottom of each page (to include each segment of messages printed on perforated paper) with its security classification, and labeled to show all applicable SCI caveats, codewords and product designators, and any DCID 1/7 control markings that apply. These markings shall be clearly shown consistent with the design of the message format being used, except that the overall

classification and applicable SCI caveat or codeword(s) and product indicator(s), and DCID 1/7 control markings shall precede the text of the message. Paragraph 21 on declassification marking and paragraph 24 on portion marking shall be applied in the case of record SCI traffic.

e. ***Files, Folders, or Groups of Documents.*** Files, folders or groups of documents shall be conspicuously marked to assure the protection of all SCI contained therein. Such material shall be marked on the file folder tab or other prominent location or affixed to an appropriate SCI cover sheet.

28. **Cover Sheets.** When it is necessary to guard against unauthorized disclosure to persons not possessing appropriate SCI accesses, separate cover sheets shall be used. Cover sheets shall show, by color or other immediately recognizable format or legend, what SCI control system, or combination of systems, they apply to, and other applicable markings.

29. **SCI Accountability and Control Procedures.** Each SCIF shall maintain systems of accountability sufficient to provide for the security of SCI disseminated, received or retained by its activity, and to assist in the investigation of compromises of SCI documents.

a. Records.

(1) *Records for Incoming SCI.* Except as provided in b below, a record shall be kept of all SCI documents received by a SCIF for at least 6 months after receipt of the material, or longer, as determined by the holding agency. Records shall identify the material by control and copy number (if used), originator, a brief description of the material, and the identity of office(s) within the SCIF that received the material. This will normally be satisfied by keeping copies of receipts or other records that provide necessary identifying data. For electrically received record traffic, this requirement may be fulfilled through retention of standard telecommunications center records for at least 6 months.

Subsequent to this process, no further accountability records or administrative controls (e.g., internal receipting among activities in the same SCIF, access records, destruction certificates) are necessary for SCI security purposes while SCI documents are maintained in or accountable to a receiving SCIF.

(2) *Outgoing SCI.* Except as provided in b below, a receipt shall be retained and a record kept for all SCI physically dispatched from the SCI for the preceding 2-year period. Receipts shall identify the material by control and copy number (if used) and originator, shall contain a brief description of the material, and identify the recipient. For Confidential COMINT-related material, this requirement may be fulfilled through the required Armed Forces Courier Service (ARFCOS) pouch or package receipt or by other appropriate dissemination records kept by the sender.

b. Raw Intelligence Data. Accountability records are not required for raw intelligence data that are transmitted from a collection point or facility to a processing facility or are being processed into a form suitable for analytical use, provided such data remain under the control of a single Intelligence Community organization, are transmitted only means authorized herein for SCI, and are accessible only to personnel meeting standards for, and granted access to, the SCI programs or control systems involved in the data.

c. Working Material. Accountability records are not required for SCI working materials used exclusively within a SCIF. Examples include preliminary drafts of papers, film chips in analysts' reference files, analyst transmissions, data base inquiries, and waste materials such

as carbon paper and stenographic notes. However, such materials must be safeguarded according to the handling, storage and disposition requirements for SCI documents.

30. **Temporary Release of SCI Outside a SCIF.** When operational needs require SCI to be released for processing or temporary use by SCI-indoctrinated persons in non-SCI accredited areas, such release shall only be accomplished with the consent and under the supervision of the responsible SCI security/control officer. The responsible officer shall obtain signed receipts for SCI released in this manner and shall ensure that conditions of use of the released material will provide adequate security until the SCI is returned to a SCIF.

31. **Audits and Inventories.** SOICs shall arrange for the conduct, by SCI security/control officers, of such periodic reviews of SCI held by organizations under their cognizance as will ensure that proper accountability is being maintained and that SCI is destroyed when no longer needed. SOICs and SCI Program Managers may require the inventory of specified SCI within activities under their cognizance.

32. **Reproduction.** Reproduction of SCI documents shall be kept to a minimum consistent with operational necessity. Copies of documents are subject to the same control, accountability, and destruction procedures as are the originals. Stated prohibitions against reproduction shall be honored. Equipment used for SCI reproduction shall be thoroughly inspected and sanitized before being removed from a SCIF.

33. **Transportation/Transmission.** SCI may be transmitted from one SCIF to another in a manner which ensures that it is properly protected.

a. ***Courier Procedures.*** SCI may be carried from one SCIF to another by two couriers approved for this purpose, by diplomatic pouch, or by ARFCOS. Courier procedures shall ensure that SCI materials are adequately protected (to the extent possible) against the possibility of hijacking, loss, exposure to unauthorized persons, or other forms of compromise.

SCI couriers must be active-duty miliary or US Government civilian employees meeting DCID 1/14 standards who are specifically designated for that purpose. Contractors and consultants are prohibited from couriering SCI unless they have been specifically approved for such duty for a particular period by the responsible SOIC.

SCI may be carried by a single officially designated courier within US Government or military installations or between SCIFs in the Washington, DC, metropolitan area. Additionally, the responsible SOIC may waive the two-courier requirement in other areas, as appropriate. Material carried by a single courier shall be transported in a securely locked briefcase or sealed pouch marked "TO BE RETURNED UNOPENED TO *(name of apppropriate organization and telephone number which will be manned at all times)* ." No inner wrapper or container is required under these circumstances.

b. ***Wrapping Procedures.*** SCI shall be enclosed for couriering in two opaque envelopes or be otherwise suitably double-wrapped using canvas bags, cartons, leather or plastic pouches, or similar containers (see a above for exception). Outer containers shall be secured with tape, lead seals, tumbler padlocks, or other means which would reasonably protect against surreptitious access. The inner and outer containers shall be annotated to show the package number and addresses of the sending and receiving SCIF. The notation "TO BE OPENED BY THE *(appropriate SCI Special Security/Control Officer)* " shall be placed above the pouch address of the receiving SCIF on both containers. The inner wrapper shall contain the document receipt and the name of the person or activity for whom the material is intended.

The applicable security classification and legend "CONTAINS SENSITIVE COMPARTMENTED INFORMATION" shall appear on each side of the inner wrapper only.

c. ***Electrical Transmissions.*** Senders of SCI transmitted electrically or electronically (to include facsimile, computer, secure voice or any other means of telecommunication) must ensure that such transmissions are made only to authorized recipients. Receivers must provide proper protection for SCI so received. Electrical transmission of SCI shall be limited to specifically designated and accredited communications circuits secured by an NSA-approved cryptographic system and/or protected distribution systems. The construction and protection of SCI telecommunications facilities shall be as prescribed in NFIB/NFIC-9.1/47 and the effective edition of KAG-1 and superseding NACSI 4000-series publications.

34. **Destruction of SCI.** SCI shall be retained for the time periods specified in records control schedules approved by the Archivist of the United States (44 U.S.C. 33 and FPMR 101-11.4). Duplicate information and other nonrecorded copies of SCI documents shall be destroyed as soon as possible after their purpose has been served. Destruction shall be accomplished in a manner that will preclude reconstruction in intelligible form. Only those methods (e.g., burning, pulping, shredding, pulverizing, melting, or chemical decomposition, depending on the type of materials to be destroyed) specifically authorized by the responsible SOIC may be used. Destruction shall be supervised and witnessed by at least two SCI-indoctrinated persons. SCI in computer or automated data processing systems or other magnetic media shall be "destroyed" through erasure by approved degaussing equipment or by executing sanitization procedures specified in the DCI's "Intelligence Community Policy for the Release of Magnetic Storage Media," 13 March 1974.

RELEASE OF SCI TO CONTRACTORS/CONSULTANTS

35. **Policy.** Basic DCI policy on release of foreign intelligence to contractors and consultants (hereafter referred to as contractors) is contained in the attachment to DCID 1/7, "DCI Policy on Release of Intelligence Information to Contractors and Consultants." SCI may be released by SOICs or their designated representatives to US Government contractors according to the following instructions. SOICs may impose more stringent requirements.

a. The release, control, handling, accountability, and destruction of SCI shall be accomplished pursuant to the provisions of the attachment to DCID 1/7 and this manual.

b. The permission of the originator of the information to be released shall be secured. (This permission may be granted in the form of lateral agreements between departments and agencies.)

c. The sponsoring agency or department shall prescribe as part of the contractual arrangement the minimum security requirements for safeguarding SCI according to this Directive. This may include a requirement that the contractor or consultant establish and maintain SCIF(s). All activities involving SCI (including discussions) shall be conducted in a SCIF.

d. SOICs of the sponsoring agency or department or their designated security representative shall perform or have performed a security survey at the contractor or consultant SCIF prior to release of SCI. The purpose of the survey is to determine that the SCIF and security procedures established by the contractor or consultant are adequate for the protection of SCI. Thereafter, periodic security inspections to ensure continuous compliance with SCI security requirements shall be conducted.

e. Decisions on selection of contractors for prospective release must take into account the potential recipients' past record in properly safeguarding classified material.

f. SCIFs established in industry must be closely monitored by the sponsoring SOIC to ensure that SCI security procedures are followed and that SCI documents are properly segregated from other materials held by the contractor. When two or more organizations release SCI to a given contractor, the organizations involved shall agree on matters of joint SCI security responsibilities.

36. **Foreign Ownership/Dominance.** Contractor companies under foreign ownership, control, or influence shall generally be ineligible for access to SCI activities and information. Foreign ownership, control, or influence in this instance means that foreign interests own five percent or more of a contractor's voting stock, or they are able through lesser holdings to control or influence the appointment and tenure of the contractor's managing officials. The responsible SOIC may waive this provision, however, if a review of the circumstances determines that the following conditions apply: the foreign ownership, control, or influence does not involve Communist countries or countries otherwise inimical to the United States, and the foreign interests do not have the right to control or influence the appointment or tenure of a contractor's managing officials. Before a waiver is granted, provision must be made to ensure that security safeguards exist to prevent disclosure of SCI to any non-US owners and managing officials. Should foreign ownership increase beyond five percent during the course of a contract, a review of the contractor's eligibility for continued access shall be made by the responsible SOIC.

LEGISLATIVE BRANCH ACCESS TO SCI

37. **Policy.**

a. As an underlying principle, access to intelligence information shall be consistent with the protection of intelligence sources and methods. Normally, Congressional requests for intelligence information can be satisfied at the collateral (i.e., non-SCI) level, but, in certain instances, there may be a need for access to SCI. In these instances, every effort shall be made to exclude, to the extent possible, data on intelligence sources and methods.

b. Members of Congress may be provided access to SCI on a need-to-know basis without a security investigation or adjudication. Heads of organizations within the Intelligence Community or program managers providing SCI shall provide briefings on the sensitivity and vulnerability of the information, and the sources and methods involved, as required to ensure proper protection.

c. Access to SCI by staff members of the Senate Select Committee on Intelligence (SSCI) and the House Permanent Select Committee on Intelligence (HPSCI) are governed by Memoranda of Understanding (MOU) executed by the Chairmen of these Committees and the DCI. Provision of information and materials to these Committees shall be in accordance with mutually agreed upon existing arrangements with the Committees.

d. Requests for SCI access approvals for other Legislative Branch personnel shall be referred to the Chief of Legislative Liaison for DCI approval. Requests must be in writing by committee or subcommittee chairmen and clearly describe the nominee's need-to-know. Issues arising with regard to particular requests shall be referred to the DCI for resolution.

Unless otherwse authorized by the DCI, approval for SCI access for Legislative Branch staff personnel shall be limited to:

(1) permanent staff personnel of appropriate Congressional committees and subcommittees;

(2) selected employees of the General Accounting Office and the Library of Congress; and

(3) selected members of the staffs of the Leadership of the House and Senate, as agreed by the DCI and the Leadership.

38. **Verification Requirement.** The DCI's Chief of Legislative Liaison will verify, in coordination with program managers and on behalf of the DCI, the need of persons in the Legislative Branch, other than members of Congress, for SCI access. Verifications shall be based on such persons' job responsibilities in the following areas:

a. direct involvement in authorization legislation pertaining to Intelligence Community organizations;

b. direct involvement in appropriations legislation for Intelligence Community organizations;

c. direct involvement in reviews authorized by law of activities of Intelligence Community organizations; and

d. direct involvement in other legislative matters which, of necessity, require direct SCI access.

39. **Access Approval procedures.**

a. SCI access approvals may be granted to staff personnel in the Legislative Branch, described above, who possess a Top Secret collateral clearance and who meet the investigative standards set forth in DCID 1/14. Requests for exceptions to this policy shall be referred to the DCI's Chief of Legislative Liaison. The requester of the SCI access approval is responsible for assuring the conduct of an appropriate investigation. Reports of investigation shall be reviewed by the CIA Director of Security to assure uniform application of DCID 1/14 security criteria. The granting of access approvals shall be coordinated with the appropriate program managers, as agreed by the DCI.

b. Staff personnel in the Legislative Branch receiving SCI access approvals shall be provided appropriate security briefings by the CIA Special Security Center and shall sign NdAs before receiving SCI access. SCI access approvals shall be recorded in the 4C system (paragraph 8). Copies of NdAs shall be provided to program managers who request them.

c. The DCI's Chief of Legislative Liaison shall be notified promptly of employee job changes or terminations to ensure updating of the 4C system and appropriate debriefing of the employee. SCI access approvals of Legislative Branch employees must be withdrawn or revalidated if an employee leaves the specific position for which access was authorized.

d. SCI shall be made available to committee and subcommittee members only through or under the authority of the chairman of the Congressional committee or subcommittee concerned.

40. **Handling and Storage of SCI.**

a. Any Intelligence Community organization that provides SCI to Congress shall ensure that the handling and storage of such information conforms to the requirements in

NFIB/NFIC-9.1/47 (see paragraph 12) or successor policy statements. SCIFs shall be accredited by the CIA Special Security Center. Where adequate provisions cannot be made for the handling and storage of SCI, no such information may be provided without the approval of the DCI.

b. Any Intelligence Community organization that provides testimony or briefings involving SCI to persons in the Legislative Branch shall do so according to the following security measures:

(1) A thorough physical security and audio countermeasures inspection of the room where testimony or briefing will occur must be conducted immediately before the presentation, unless the premises are maintained in a secure status. Audio countermeasures surveillance of the premises should also be maintained during the presentation, unless the premises are maintained in a secure status.

(2) All persons present, other than elected officials, including transcribers and other clerical personnel, must be certified for access to the SCI being discussed. Arrangements shall be made to monitor entrances to the room where the presentation will be given to exclude unauthorized persons.

(3) All transcriptions or notes that result from briefings or testimony must be handled and stored according to the SCI security requirements as specified in a, above.

(4) The room in which a presentation is given must be inspected after the presentation to ensure that all SCI is properly secured.

(5) Any Intelligence Community organization that provides SCI to a Congressional committee, other than a committee routinely involved in the oversight and appropriations processes of Intelligence Community organizations, shall endeavor to provide such information through the SSCI or HPSCI, as appropriate. The SSCI and HPSCI both have facilities that meet the NFIB/NFIC-9.1/47 requirements and personnel trained in SCI handling procedures. The committee requesting the information shall contact the HPSCI or SSCI and obtain their permission to use their facilities prior to the transmittal of the information. Where possible, custody of such information shall remain with the Intelligence Community organization concerned. Where such information must be physically transferred, efforts shall be made beforehand to eliminate or minimize the risk of exposure of SCI sources and methods.

41. **Marking SCI Released to Congress.** SCI being prepared for release to Members of Congress and Congressional committees shall be marked with all applicable classifications, SCI caveats, codewords, project indicators and DCID 1/7 control markings. The term "SENSITIVE" may not be used instead of, or in addition to, SCI markings. Releasing agencies shall ensure, through their legislative offices or comparable elements, that Congressional committee staff employees, and employees of the Library of Congress and the General Accounting Office, have clearances and SCI access authorizations appropriate for receipt of the material involved. Releasing agencies also shall ensure that SCI being provided Legislative Branch components is stored in accredited SCIFs.

JUDICIAL BRANCH ACCESS TO SCI

42. **Policy.** Pursuant to the Classified Information Procedures Act of 1980 (CIPA) (Public Law 96-456. 94 Stat. 2025 18 U.S.C. Appendix 4) and the "Security Procedures Established Pursuant to Public Law 96-456. 94 Stat. 2025 18 U.S.C. Appendix 4, By The Chief Justice

of the United States For The Protection of Classified Information," dated 12 February 1981, arrangements for the care, custody, and control of SCI material involved in any federal criminal case shall be the responsibility of the Department of Justice (DOJ) Security Officer in coordination with the appropriate Executive Branch agency security representative.

a. An SCI access authorization for federally appointed judges and justices is not required. If desired, however, an SCI authorization can be granted and a formal briefing presented to the requesting judge/justice through coordination with the DOJ Security Officer.

b. Magistrates, immigration commissioners, administrative law judges, hearing commissioners, and other such court officials, who are not appointed by the Federal Government, or who have not been subjects of background investigations as part of the appointment process, must obtain SCI access authorization.

c. All other court, government, or support personnel (law clerks, attorneys, US Marshals, courtroom clerks, court reporters, administrative officers, secretaries, etc.), who have a validated need-to-know, must obtain SCI access authorization.

d. The Government may obtain, consistent with the CIPA and its "Security Procedures," as much information as possible in its attempt to make an adjudication pursuant to DCID 1/14, for those individuals acting for the defense.

e. There is no requirement for investigation or SCI access authorization for members of the jury.

f. A Court Security Officer (CSO) shall be appointed by the Court from recommendations submitted by the DOJ Security Officer and with the concurrence of the head of any Intelligence Community entity (or his/her designee) from which the case-related SCI originates. The CSO is responsible for ensuring compliance with the CIPA and all other applicable directives and regulations concerning the safeguarding of SCI; and, for providing SCI security support, as needed, for all persons involved in the particular case.

43. **SCI Access Verification.** Requirements for SCI access shall be provided to the CSO who shall notify the DOJ Security Officer. The DOJ Security Officer shall coordinate requirements with agencies/program managers involved.

44. **SCI Access Eligibility Determination Procedures.** SCI access will be authorized by the DOJ Security Officer, who is responsible for adjudicating the results of investigations required by DCID 1/14.

a. The Court, and other appropriate officials, shall be notified in writing by the DOJ Security Officer of SCI access approvals.

b. SCI briefings shall be provided by DOJ Special Security Center (SSC) personnel, or by an appropriately indoctrinated representative with the DOJ SSC.

45. **Handling and Storage of SCI.** Matters pertaining to the handling, storage, and disposition of SCI shall be coordinated with the CSO who is responsible for ensuring that proper safeguarding procedures are established and that adequate storage is provided for SCI pursuant to the CIPA Security Procedures and this manual. These matters shall be coordinated with the U.S. Intelligence Community entities originating the SCI case material.

46. **Additional Details.** Additional details/information may be found in the CIPA and/or the "Security Procedures," which may be obtained from the DOJ SSC. Any question concerning the interpretation of any security requirement contained in the CIPA security procedures

shall be resolved by the Court in consultation with the DOJ Security Officer and the appropriate Executive Branch agency security representative.

SCI SECURITY VIOLATIONS/COMPROMISES

47. **Individual Responsibilities.** All possible security violations or compromises involving SCI shall be immediately reported to the applicable SCI Security/Control Officer. Immediate action shall be taken to maintain the physical security of SCI documents discovered in an insecure environment until such material can be restored to SCI control. SOICs shall ensure that persons under their cognizance are advised and periodically reminded of these responsibilities.

48. **Investigations.** SOICs shall establish procedures within their organizations to ensure that all reported actual or potential security violations or compromises occurring in areas subject to their jurisdiction are properly investigated to determine if there is a reasonable likelihood that a compromise may have occurred.

a. If so, the cognizant SOIC, or other authority designated by the SOIC, shall immediately report the incident to the appropriate Intelligence Community program manager. An investigation shall be conducted to identify full details on the violation/compromise, and to determine what specific information was involved, what damage resulted, and whether culpability was involved in the incident.

b. If the case involves an inadvertent disclosure, the SCI Security/Control Officer is expected to exercise his or her best judgment as to whether the interests of SCI security are well served by seeking written agreements from unindoctrinated persons to whom SCI has been inadvertently disclosed. If the judgment is that those interests are so served, the person(s) involved sign an inadvertent disclosure agreement, and the responsible SCI Security/Control Officer has reason to believe that the person(s) will maintain absolute secrecy over the SCI involved, the report of investigation may conclude that no compromise occurred.

c. The form of inadvertent disclosure agreement may be developed by SOICs, but shall, in all cases, be structured so that it conveys no classified information itself, emphasizes that there is no time limit on the need to safeguard the disclosed data, reminds the signer of the provisions of the Espionage Statutes, and commits the signer to certifying his or her understanding of the situation and to affirming that he or she will never, without proper authority, disclose or discuss the information with any other person.

d. When investigations show that SCI was inadvertently disclosed to foreign nationals, or that cases under investigation involve damage deemed significant by the cognizant SOIC, espionage, flagrant dereliction of security duties, or serious inadequacy of security policies and procedures, summaries of the investigations and of related actions shall be provided to the DCI by the responsible SOIC. The DCI Security Committee is the preferred channel for such reporting.

49. **Corrective Action.** Investigating oficers shall advise cognizant SOICs of weaknesses in security programs and recommend corrective action(s). SOICs are responsible for ensuring that appropriate corrective action is taken in all cases of actual security violations and compromises. Administrative sanctions imposed in cases of demonstrated culpability shall be recorded in security files of the responsible SOIC. Security deficiencies identified by investigation to have contributed directly to the incident shall be corrected if it is within the capability of the SOIC concerned; if not, full details and recommendations on corrective measures shall be provided to the DCI through the DCI Security Committee.

INSPECTIONS

50. **Policy.** Periodic inspections of SCIFs by the responsible SOIC are mandatory. Inspections shall be performed by persons knowledgeable of SCI storage, control, and protection procedures and shall be designed to ensure that procedures and safeguards comply with the requirements of NFIB/NFIC-9.1/47, this manual, and other applicable directives. Inspection reports shall be retained in the files of the accrediting organization. Intelligence Community organization inspection reports of joint SCIFs may be accepted by any other organization which uses the SCIF as valid findings of the degree of compliance with applicable security standards. Inspection reports shall identify any deficiencies found and the status of actions taken to correct them.