DIRECTOR OF CENTRAL INTELLIGENCE

SENSITIVE COMPARTMENTED INFORMATION SECURITY REGULATION

(Attachment to DCID 1/19, "Uniform Procedures for Administrative Handling and Accountability of Sensitive Compartmented Information (SCI)")

Table of Contents

SENSITIVE COMPARTMENTED INFORMATION
SECURITY REGULATION

1. *Definitions*

a. *Sensitive Compartmented Information (SCI).* All information and material bearing special controls for restricted handling within compartmented foreign intelligence systems.

b. *Executive Agent Program.* A program wherein a single department, agency, or organization collects or processes foreign intelligence for the Intelligence Community at the direction of the DCI or higher national authority.

c. *Operational Compartment.* A compartment designed to protect policy, planning, research and development, contracting, budgeting and mission-related information pertaining to systems of foreign intelligence collection.

d. *Senior Intelligence Officer (SIOs) of the Intelligence Community.* For the purpose of this directive, this term refers to those officials who represent their departments or agencies on the National Foreign Intelligence Board (NFIB).

2. *General Procedures*

a. *Accreditation of SCI Facilities.* Before a facility is authorized to handle SCI, it must be accredited as meeting the construction and protection standards of USIB-D-9.1/20. The DCI will accredit all SCI facilities except where that authority has been specifically delegated. The accreditation shall specify which of the SCI compartments apply to each facility.

Each accrediting official shall maintain a physical security profile on facilities accredited by him to include complete details on the overall security environment as prescribed by USIB-D-9.1/20.

The Central Intelligence Agency will be responsible for accrediting those SCI facilities within organizations not under the security cognizance of an Intelligence Community SIO.

The DCI reserves the right to review all accreditation files and inspect all SCI facilities.

b. *SCI Security Control Center (SCC).* Each SCI-accredited facility shall be serviced by an SCI Security Control Center which shall be the focal point for the security, receipt, control, storage, and dissemination of SCI. In instances where it is not practical for an NFIB member to maintain a single centralized SCC, the control mechanism may be established on the basis of selected components within an agency or department. The appropriate SIO shall designate an appropriately indoctrinated person(s), and alternate thereto, to operate the Control Center. This person shall:

- Act as the exclusive control point for receiving and dispatching SCI via electrical, courier, or other means approved for the transmission of SCI.
- Complete and return to the sender all receipts attached to SCI documents received by courier/pouch.

— With other appropriate officials, insure that SCI is accounted for, controlled, transmitted, destroyed, packaged, and otherwise safeguarded according to this directive.
— Maintain an accurate and current personnel access record and ensure that SCI is disseminated only to those persons properly indoctrinated with a validated need-to-know.

Intelligence Community SIOs shall establish training programs for their SCI Control/Security Officers and other personnel engaged in the security management of SCI facilities within their departments or agencies. The scope and duration of the training shall be sufficient to ensure that personnel are adequately prepared to carry out their duties.

c. *Records.* Except as provided in Section f below, SCI-accredited facilities shall keep a record of the initial receipt and internal distribution of all SCI received, by any means, for a minimum of six months. This record must describe in detail the SCI received and be annotated to reflect which office(s) within the facility was the recipient of the SCI. Recording of incoming SCI is required regardless of geographic proximity between the sender and recipient.

d. *Receipts.* The permanent transfer of SCI among SCI-accredited facilities shall be covered by a receipt detailing individual SCI items. However, in the case of Confidential COMINT-related material, this requirement may be fulfilled through the required ARFCOS pouch or package receipt or by other appropriate dissemination records kept by the sender. Such receipts shall be retained for a minimum of two years.

e. *Accountability and Control Within an SCI-Accredited Facility.* Subsequent to the initial recording process required by subparagraph c above, no further SCI security accountability controls (for example, internal receipting, certificates of destruction, inventories, document control numbers, access records, etc.) are necessary within an SCI-accredited area. However, SIOs may impose such additional administrative controls as deemed necessary to insure efficient administration of activities under their control.

f. *Control of Raw Intelligence Data.* Raw intelligence data being transmitted from a collection point or facility to a processing facility, and while being processed into a form suitable for analytical use, need not be subject to any individual accountability controls provided it remains under the control of a single Intelligence Community agency; is transmitted only by means authorized herein for SCI; and is accessible only to personnel meeting standards for and granted access to the compartmentation programs involved in the collection and processing of such information.

g. *Audits.* SCI Control/Security Officers shall periodically review holdings of SCI to ensure that proper accountability is being maintained and that SCI is destroyed when no longer needed. SIOs and/or SCI Executive Agent Program Managers may require the inventory of specified SCI.

h. *Control Numbers.* Originators shall assign a control number to all SCI material 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 shall be assigned to Intelligence Community SIOs by CIA/Office of Security/Compartmented Information Branch.

(1) Single Control System Material. For material containing information from only one SCI control system, each control number shall consist of the letters of

the applicable SCI control system, a dash, a six-digit number selected on a "one-up" basis from the block of numbers assigned to the activity, a slant or oblique stroke, and the last two digits of the current year. For example, "BYE-123456/76," "TCS-234567/77," or "SI-345678/78."

(2) Multiple Control System Material. When the material contains information from more than one SCI control system, then the control number shall be selected according to the precedence shown in (1) above (i.e., joint BYE and TCS or SI material would reflect the appropriate BYE number ; joint TCS and SI material, a TCS number).

i. *Cover Sheets.* To preclude unauthorized disclosure, an unclassified cover sheet shall be used when transmitting SCI outside of an SCC. Publications need not have a separate document cover sheet affixed if the publication cover includes all prescribed markings and is unclassified standing alone.

j. *Transmission.* The transmission of SCI shall be restricted to means specifically approved and accredited by the DCI for this purpose.

(1) Electrical. Electrical transmission of SCI shall be limited to specifically designated communications circuits secured by an NSA-approved crypto system or protected distribution system.

The construction and protection of SCI communications facilities shall be as prescribed in ~~USIB-D-9.1/20~~, and the effective edition of KAG-1 communications policy and procedures.

Operational procedures shall ensure that only properly indoctrinated personnel are provided access to clear text SCI.

All automated data processing of SCI shall be according to standards prescribed in DCID 1/16.

SCI transmitted electronically will be controlled according to procedures prescribed in this Security Regulation. Senders must assure that electronic transmissions are made only to authorized recipients and receivers must provide procedures for the proper protection of SCI received in this manner. These procedures shall include the establishment of a recipent's need-to-know in circumstances where no hard copy or record copy of the material will result.

All electronic equipment which is used to process or transmit any SCI shall meet national standards for TEMPEST.

(2) Non-Electrical. SCI shall be transmitted from one SCI facility to another by two SCI couriers approved for this purpose, by diplomatic pouch, or by Armed Forces Courier Service (ARFCOS). Courier procedures shall ensure that SCI materials are adequately protected against the possibility of hijacking, unauthorized viewing, loss, or other form of compromise during the transmission. Transmittal of SCI via commercial aircraft not under U.S. Government or military charter is prohibited.* The Departmental SIO must specifically approve all exceptions.

SCI couriers shall be active duty military or U.S. Government civilian employees meeting DCID 1/14 standards and be specifically designated by the responsible SIO. Couriering of SCI by contractor employees is prohibited except when specifically approved by an Inteligence Community SIO or an Executive Agent/Operational Program Manager.

* Does not apply to ARFCOS and the diplomatic courier service.

SCI materials shall be enclosed for delivery in two opaque envelopes or otherwise be suitably double-wrapped using canvas bags, cartons, crates, leather pouches, etc. Containers will be secured with tape, lead seals, tumbler padlocks, or by other means which would reasonably protect against surreptitious access to SCI materials.

The inner and outer container shall be annotated to show the pouch address and package number of the sending SCI facility. The notation "TO BE OPENED BY THE (SSO, TCO, BCO)" shall be placed above the pouch address of the receiving SCI facility on both containers. The proper security classification and caveat "CONTAINS SENSITIVE COMPARTMENTED INFORMATION" shall be annotated on each side of the inner wrapper only. The inner container shall contain the document receipt and should also reflect the name or office symbol of the person/activity for whom the material is intended.

SCI documents may be transported by officially designated couriers within U.S. Government or Military Installations and within the Washington D.C. Metropolitan area in a securely locked briefcase or sealed pouch marked "TO BE RETURNED UNOPENED TO (Name of SCI Facility)" and other applicable information. No inner wrapper or container is required under these circumstances.

k. *Destruction.* As soon as possible after its purpose has been served, all SCI shall be destroyed in a manner that will preclude reconstruction in any intelligible form. Only those methods (these may include burning, pulping, pulverizing, melting or chemical decomposition, depending on the type of SCI materials to be destroyed) specifically authorized by the responsible SIO shall be used. Destruction shall be supervised and witnessed by at least two SCI indoctrinated individuals. SCI contained within computer or automated data processing systems or other magnetic media shall be erased by approved degaussing equipment or by other means designated by the DCI.

l. *Control of SCI Temporarily Released to Non-SCI-Accredited Areas.* Necessity may require processing or the temporary release of SCI to SCI-indoctrinated persons located in non-SCI-accredited areas.

Such usage shall be authorized only with the express consent and direct supervision of the local Security Control Center Officer who shall obtain a signed receipt for the SCI documents and otherwise insure that proper SCI security is maintained until the documents are returned to an SCI-accredited area.

The temporary release of SCI shall not extend beyond the normal duty day.

m. *Reproduction.* Reproduction of SCI shall be kept to a minimum consistent with operational necessity. Copies of documents are subject to the same controls as the original. Adherence to stated prohibitions against reproduction is mandatory. Any equipment used for SCI reproduction must be thoroughly inspected and sanitized before removal from an SCI facility.

3. *Classification and Marking of Documents and Materials*

a. *Classification, Codewords, Designators, and Caveats.* Assignment of classification, system codewords, designators, and caveats shall be in accordance with guidance promulgated by officials responsible for each individual SCI control system, executive agent program, or operational compartment and concurred in by the DCI. All classification guidance shall be in accord with the policies and procedures of Executive Order 11652.

b. *Overall and Page Marking.* The overall classification of an SCI document, whether or not permanently bound, or any copy or reproduction thereof, shall be

conspicuously marked or stamped at the top and bottom on the outside of the front cover (if any), on the title page (if any), on the first page, on the back page, and on the outside of the back cover (if any). Each interior page of a document shall be conspicuously marked or stamped at the top and bottom with the highest classification of information appearing thereon, including the designation "Unclassified" when appropriate.

c. *Control System Caveats.* The SCI Control System caveat (i.e., "HANDLE VIA (Name of SCI Control System) CONTROL CHANNELS") shall be annotated on the front cover, title page, back cover, and first page. Each interior page which contains information requiring SCI protection shall be marked with the classification and codeword, caveat or designator as appropriate. If the document contains information from more than one SCI control system, then add the word "JOINTLY" to the caveat. The SCI control system caveat shall normally appear at the bottom right of the page.

d. *Control Number.* The SCI Control Number (if required according to paragraph 2h) shall be placed immediately above the SCI control system caveat on the front cover and title page.

e. *Codewords and Executive Agent Program Operational Designators.* SCI codewords and designators shall be annotated on the top and bottom of the title page, first page, and each page which contains information requiring codeword/designator protection.

f. *Control Markings for the Dissemination of Foreign Intelligence and Related Material.* Restrictive and other markings prescribed in DCID 1/7 shall be used on the title page, front cover, and other applicable pages or paragraphs when it is necessary to control the dissemination of foreign intelligence or related material which also requires SCI protection.

g. *Markings for SCI to be Furnished to Persons Outside the Executive Branch of the Government.* When SCI is furnished to persons outside the Executive Branch of the Government, the warning notice "NATIONAL SECURITY INFORMATION—UNAUTHORIZED DISCLOSURE SUBJECT TO CRIMINAL SANCTIONS" shall be placed on the front cover and title page.

h. *Exemption from General Declassification Schedule.* All SCI is exempt from the General Declassification Schedule of Executive Order 11652. The following exemption notification shall be used on the cover, title page, or first page of typescript text, or inside cover of formal publications:

CLASSIFIED BY (APPROPRIATE AUTHORITY)
EXEMPT FROM GENERAL DECLASSIFICATION
SCHEDULE OF EXECUTIVE ORDER 11652
EXEMPTION CATEGORY SECTION 5B(2)
DECLASSIFY UPON NOTIFICATION BY ORIGINATOR

The abbreviation "XGDS (2) (UNO) may be substituted in electrically transmitted messages and in similarly appropriate circumstances.

i. *Transmittal Documents.*

(1) SCI Transmittal Documents. When transmittal documents contain SCI, they shall bear the highest necessary classification, codewords, designators, and caveats. When the transmittal document is of a different classification or SCI category than the material being transmitted, the following notation shall be applied: "REGRADE AS (CLASSIFICATION, CODEWORD,

ETC.) WHEN APPENDED SCI DOCUMENTS ARE REMOVED." Inappropriate codewords, caveats, and designators must be physically removed.

(2) Non-SCI Transmittal Documents. When a non-SCI transmittal document serves to transmit SCI material, it shall bear the highest classification of the material being transmitted and an unclassified caveat stating "CONTAINS (SI/TK/B/OTHER) INFORMATION." Classified codewords and caveats shall not be used on non-SCI transmittal documents. When the transmittal document is unclassified or of a lower classification than the material being transmitted, the following notation shall be applied: "REGRADE AS (CLASSIFICATION) WHEN APPENDED SCI DOCUMENTS ARE REMOVED."

j. *Marking Document Components.* In some complex documents, its major components (i.e., annex, chapter, appendix, or attachment) are likely to be used separately. In such cases, each component shall be marked as a separate document according to content.

To the extent practicable, paragraphs, subparagraphs, titles, or other internal document components shall be marked to show the level of classification, system control caveats, and dissemination control markings, if any, or that the component is unclassified.

k. *Marking Magnetic Media.* To facilitate identification, accounting, and control of SCI in magnetic form, each reel or cassette of tape, each magnetic card, or disk pack shall be promptly marked with a label which includes the SCI control system markings, security classification, and other required markings or caveats. Internal media identification must include, as a minimum, both a header and trailer block which contains the labeling data of the external security markings.

l. *Marking Photographic Material in Roll Form.* To facilitate the identification, accounting, and control of SCI film in roll form, labels shall be used which include the SCI control system markings, security classification, and other required markings or caveats.

Labels on roll film placed in metal containers shall be located as follows: (1) one on the end of the spool flange, (2) one on the side of the spool container, and (3) one on the container cover.

Film in plastic containers with clear plastic covers need only one label, placed on the spool flange. This is to facilitate reuse of the plastic container.

The film itself shall include all required SCI control system markings on the head and tail identifications.

m. *Marking Microform Material.*

(1) Microfiche. Each microfiche will have a heading whose elements are readable without magnification. The heading elements will specify: the long and short titles of the document; security classification and codewords which shall not be abbreviated; standard abbreviations or codes for handling caveats, dissemination control markings and distribution restrictions. If the microfiche is intended for exchange among NFIB agencies, the exact placement of the heading elements will be in accordance with "DCI Standards for Microfiche Copies of Intelligence Documents, May 1977." Microfiche may also be placed in envelopes which, through a color code

specified in the above mentioned DCI Standard, indicate the level of security protection to be accorded the microfiche.

(2) Microfilm. Each roll of microfilm, whether mounted on an open reel or in a cartridge, will contain security information which is readable without magnification. For source document microfilm, the information will be on a page target containing the security classification and codewords which shall not be abbreviated; standard abbreviations and codes for handling caveats, dissemination control markings and distribution restrictions. This page target will immediately precede the first page of the document and will follow the last page of text preceding the "END—date filmed" target frame. For film produced by a Computer Output Microfilm (COM) recorder, the above mentioned security information will be recorded in human readable format when within equipment capability on a length of film immediately preceding and following the document text. The boxes containing processed film on open reels and the film cartridges will be labeled with the appropriate security information. In addition, the labeling will include the document long and short titles.

n. *Marking 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.

o. *Marking Abbreviations.* Distinctive SCI control system designators, codewords, caveats, etc., shall not be abbreviated when there is any likelihood that the abbreviations will be confused or otherwise not understood by the recipient.

p. *Marking Electrically Transmitted SCI Messages.* SCI transmitted by accredited communications circuits or other specialized means shall be marked at the top and bottom with the assigned classification and paragraph marked in the manner prescribed above for documents. Applicable SCI codewords, designators, caveats, etc., shall be clearly shown consistent with the design of the message form or format being used.

The first item in the text of an SCI message shall be the overall classification of the message, applicable SCI codeword(s)/Executive Agent Program Operational Designator, SCI Control System Designator, and such other markings as may be required by DCID 1/7.

4. *Minimum Standards for Control of SCI Released to Contractors or Consultants*

SCI may be released (release is defined as the visual, oral, or physical disclosure of SCI) by NFIB members or their designated representatives (includng military departments) to United States Government contractors or consultants provided that:

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

— The sponsoring agency ensures that such releases are made according to the provisions of this directive.

— The sponsoring agency maintains appropriate records of the SCI material released to contractors or consultants.

— The sponsoring agency or department shall prescribe as part of the contractual arrangement the minimum security requirements for safeguarding SCI in accordance with this directive. This shall include a requirement that the contractor or consultant establish and maintain SCI secure areas according to USIB-D-9.1/20 standards. All activities involving SCI materials for information (including discussions) shall be conducted therein.

— The head of the sponsoring agency or department or his designated security representative shall perform or have performed a security survey and provide formal accreditation for the appropriate SCI program at the contractor or consultant facility prior to physical release of SCI. The purpose of the survey is to determine that the physical plant and security procedures established by the contractor or consultant meet all standards for the protection of SCI. Thereafter, periodic security inspections to ensure continuous compliance with physical security requirements shall be conducted.

— Contractor or consultant personnel shall be certified as having a need-to-know for SCI access by the sponsoring agency and as being cleared and indoctrinated for SCI according to criteria and procedures established in DCID 1/14.

— Contractors and consultants shall be required to maintain such records as to account for all SCI materials received, disposed of, produced and maintained by them for the duration of the contract and to permit identification of all individuals who have had access to SCI in their custody.

— Contractors or consultants receiving releases of SCI do not release the material to any activity or individual of the contractor or consultant organization not directly engaged in providing services under the contract or agreement nor to any other contractor or consultant (including a subcontractor) without the consent of the sponsoring agency (which shall verify that the second contractor has a need-to-know and meets security requirements).

— Contractors or consultants do not reproduce any SCI without the permission of the sponsoring agency. Such material shall be classified, controlled, and accounted for in the same manner as the originals.

— Contractors or consultants do not destroy any SCI material without the permission of the sponsoring agency. When destruction is authorized, it is subject to the provisions of paragraph 2k above and a record of destruction must be maintained.

— SCI or information related to SCI is not released to foreign nationals whether or not they are also consultants, U.S. contractors or employees thereof, regardless of the level of their security clearance, except with the permission of the originating agency.

— SCI or information related to SCI released to a contractor or consultant does not become the property of the contractor or consultant and can be withdrawn at the discretion of the sponsoring agency. Upon expiration of the sponsoring agency shall make provision for: (a) return of all SCI materials and all other materials related to or incorporating data from such SCI materials in the hands of the contractor or consultant to the sponsoring

ILLEGIB

agency; or (b) retention of that SCI or related SCI material, when specifically required, by the contractor or consultant, provided that the requisite security safeguards and accountability procedures specified by this directive continue to be maintained by the contractor or consultant.