28 October 1981

D R A F T

PROPOSED CHANGES TO DCID 1/14

DIRECTOR OF CENTRAL INTELLIGENCE DIRECTIVE NO. 1/14[1]

MINIMUM PERSONNEL SECURITY STANDARDS AND PROCEDURES GOVERNING ELIGIBILITY FOR ACCESS TO SENSITIVE COMPARTMENTED INFORMATION

(1) (Effective _____)

(2) Pursuant to the provisions of Executive Order ~~12065~~ 12036 and 12065, Section 102 of the National Security Act of 1947 and National Security Council Directives, the following minimum personnel security standards, procedures and continuing security programs are hereby established for all United States Government civilian and military personnel, consultants, contractors, employees of contractors and other individuals who require access to Sensitive Compartmented Information[2] (hereinafter referred to as SCI). The standards, procedures and programs established herein are minimum and the departments and agencies may establish such additional security steps as may be deemed necessary and appropriate to ensure that effective security is maintained.

Purpose

1. The purpose of this Directive is to enhance the security protection of SCI through the application of minimum security standards, procedures and continuing security programs, and to facilitate the security certification process among Government departments and agencies.

Applicability

2. The provisions of the Directive shall apply to all persons (other than elected officials of the United States Government, federal judges and those individuals for whom the DCI makes a specific exception) without regard to civilian or military status, form of employment, official rank or position or length of service.

3. Individuals who do not meet the minimum security criteria contained herein and who are, therefore, denied access to SCI shall not, solely, for this reason, be considered ineligible for access to other classified information. Individuals whose access to SCI has been authorized as an exception granted in accordance with (3) paragraph 76 below, shall not, solely for that reason, be considered eligible for access to other classified information.

---

(4) [1]This directive supersedes DCID 1/14 approved 13 May 1976.

[2]The term "Sensitive Compartmented Information" as used in this Directive is intended to include all information and materials bearing special community controls indicating restricted handling within present and future community intelligence collection programs and their end products for which community systems of compartmentation have been or will be formally established. The term does not include Restricted Data as defined in Section II Public Laws 585, Atomic Energy Act of 1954, as amended.

General

4. The granting of access to SCI shall be controlled under the strictest application of the "need-to-know" principle under procedures prescribed in the several existing authorities which govern access thereto, and in accordance with the personnel security standards and procedures set forth in this Directive. All persons accountable under the authority of this Directive and given access to information (SCI) containing sources or methods of intelligence shall, as a condition of obtaining access, sign an agreement that they will not disclose that information to persons not authorized to receive it.

Personnel Security Standards

5. Criteria for security approval of an individual on a need-to-know basis for access to SCI are as follows:

(5) a. The individual shall be stable, trustworthy, reliable, of excellent character and discretion and of unquestioned loyalty to the United States.

(6) b. Except where there is a compelling need, and a determination has been made by competent authority as described in paragraph 76 below that every reasonable assurance has been obtained that under the circumstances the security risk is negligible:

(7) (8) (1) Both the individual and the members of his or her immediate family shall be U.S. citizens. For these purposes, "immediate family" ~~is defined as including~~ includes the individual's spouse, parents, brothers, sisters and children.*

(9) (10) (2) The members of the individual's immediate family and persons to whom he or she is bound by affection or obligation** should neither be subject to physical, mental or other forms of duress by a foreign power, nor advocate the use of force or violence to overthrow the Government of the United States or the alteration of the form of Government of the United States by unconstitutional means.

(11) Exceptions to Personnel Security Standards

(12) 6. The exceptions to paragraph 5.b.(1) (2) above may be granted only by the Senior Intelligence Officer (SIO) of the Intelligence Community organization or his designee unless such authority has been specifically delegated to the head of an office or organization as set forth in interdepartmental agreements. All exceptions granted will be common sense determinations based on all available information, and shall be recorded by the agency making the exception. In those cases in which the individual has lived outside of the United States for a substantial period of his life, a thorough assessment of the adequacy of the investigation in terms of fulfillment of the minimum investigative requirements, and judicious review of the information therein must be made before an exception is considered.

-8- *The requirement for U.S. citizenship in this DCID also applies to a cohabitant.

-10- **Including a cohabitant.

Investigative Requirements

7. The investigation conducted on an individual under consideration for access to SCI will be thorough and shall be designed to develop information as to whether the individual clearly meets the above Personnel Security Standards.

8. The investigation shall be accomplished through record checks and personal interviews of various sources by trained investigative personnel in order to establish affirmatively to the adjudicating agency complete continuity of identity to include birth, residences, education, employment and military service. Where the circumstances of a case indicate, the investigation shall exceed the basic requirements set out below to ensure that those responsible for adjudicating access eligibility have in their possession all the relevant facts available.

9. The individual shall furnish a signed personal history statement, fingerprints of a quality acceptable to the Federal Bureau of Investigation and a signed release, as necessary, authorizing custodians of police, credit, education and medical records, to provide record information to the investigative agency. Photographs of the individual shall also be obtained where additional corroboration of identity is required.

10. Minimum standards for the investigation are as follows:

a. Verification of date and place of birth and citizenship.

b. Check of the subversive and criminal files of the Federal Bureau of Investigation, including submission of fingerprint charts, and such other National agencies as are appropriate to the individual's background. An additional check of Immigration and Naturalization Service records shall be conducted on those members of the individual's immediate family who are United States citizens other than by birth or who are resident aliens.

c. A check of appropriate police records covering all areas ~~where the individual has resided~~ of the individual's residences, employment and education in the U.S. throughout the most recent fifteen (15) years or since age eighteen, whichever is the shorter period.

d. Verification of the individual's financial status and credit habits through checks of appropriate credit institutions and/or interviews with knowledgeable sources covering all areas of employment, residence, and education in the most recent ~~five (5)~~ seven (7) years.

e. Interviews with neighbors in the vicinity of all the individual's residences in excess of six (6) months throughout the most recent five (5) year period. This coverage shall be expanded where the investigation suggests the existence of some questionable behavioral pattern.

f. Confirmation of all employment during the past fifteen (15) years or since age eighteen, whichever is the shorter period, but in any event the most recent two (2) years. Personal interviews with supervisors and co-workers at places of employment covering the past ten (10) years shall be accomplished.

17 g. Verification of graduation or attendance at all institutions of higher learning within the past fifteen (15) years. If individual did not attend an institution of higher learning, verification of graduation or attendance at last secondary school within the past ten (10) years.

~~Attendance at secondary schools may be verified through qualified collateral sources. If attendance at educational institutions occurred within the most recent five (5) years, personal interviews with faculty members or other persons who were acquainted with the individual during his attendance shall be accomplished.~~

h. Review of appropriate military records.

i. Interviews with a sufficient number of knowledgeable
18 sources ~~acquaintances~~ (a minimum of three developed during
the course of the investigation) as necessary to provide a
continuity to the extent practicable, of the individual's
activities and behavioral patterns over the past fifteen (15)
years. ~~with particular emphasis on the most recent five (5)~~
19 ~~years~~.

j. When employment, education or residence has
occurred overseas (except for periods of less than ~~five (5)~~
20 ~~years~~ one year for personnel on U.S. Government assignment
and less than ninety days for other purposes) during the past
fifteen (15) years or since age eighteen, a check of the
21 records will be made at the Department of State and/ or
other appropriate agencies. Efforts shall be made to
develop sources, generally in the United States, who knew
the individual overseas in order to cover significant
employment, education or residence and to attempt to determine if any lasting foreign contacts or connections were
established during this period. However, in all cases
where an individual has worked or lived outside of the
U.S. continuously for over ~~five (5) years~~ one year, the
22 investigation will be expanded to cover fully this period
in his life through the use of such investigative assets
and checks of record sources as may be available to the
U.S. Government in the foreign country(ies) in which the
individual resided.

23 k. ~~In those instances in which~~ When the individual has immediate family members or other persons ~~with~~ to whom ~~he~~ the individual is bound by affection or obligation in any of the situations described in subparagraph 5.b.(2), above, the investigation will include an interview of the individual by trained security, investigative or counterintelligence personnel to ascertain the facts as they may relate to the individual's access eligibility.

l. In all cases, the individual's spouse or cohabi-
24 tant shall at a minimum be checked through the subversive
and criminal files of the Federal Bureau of Investigation
and other National agencies as appropriate. When conditions
indicate, additional investigation shall be conducted on the
spouse of the individual and members of the immediate family
(or other persons to whom the individual is bound by affec-
25 tion or obligation) to the extent necessary to permit a
determination by the adjudicating agency that the provisions
of paragraph 5 (Personnel Security Standards) above are met
26 (See Annex A).

m. A personal interview of the individual will be conducted by trained security, investigative or counterintelligence personnel when necessary to resolve any significant adverse information and/or inconsistencies developed during the investigation.

Exceptions to Investigative Requirements

11. (Old Paragraph 6) In exceptional cases, the Senior Intelligence Officer of the Intelligence Community Organization, the SIO or his designee may determine that it is necessary or advisable in the National interest to authorize access to SCI prior to completion of the fully prescribed investigation noted in paragraph 10 above. In this situation, such investigative checks as are immediately possible shall be made at once and should shall include a personal interview of the individual by trained security, investigative, or counterintelligence personnel. Access in such cases shall be strictly controlled and the fully prescribed investigation and final evaluation shall be completed at the earliest practicable moment. Certification to other organizations of individuals authorized access in such cases shall include explicit notification of the exception.

12. Where a previous investigation has been conducted within the past five (5) years which substantially meets the above minimum standards, it may serve as a basis for granting access approval provided a review of the personnel and security files does not reveal substantive changes in the individual's security eligibility. If a previous investigation does not substantially meet the minimum standards or if it is more than five (5) years old, a current investigation shall be required but may be limited to that necessary to bring the individual's file up-to-date in accordance with the investigative requirements set forth in paragraph 10 above. Should new information be developed during the current investigation which bears unfavorably upon the individual's activities covered by the previous investigation, the current inquiries shall be expanded as necessary to develop full details of this new information.

Periodic Reinvestigations

13. Programs shall be instituted requiring the periodic reinvestigation of personnel provided access to SCI. These reinvestigations shall be conducted on a five (5) year recurrent basis, but on a more frequent basis where the individual has shown some questionable behavioral pattern, his activities are otherwise suspect, or when deemed necessary by the SIO concerned.*

14. The scope of reinvestigations shall be determined by the SIO concerned based on such considerations as the potential damage that might result from the individual's defection or willful compromise of SCI and the availability and probable effectiveness of other means to continually evaluate factors related to the individual's suitability for continued access. The individual shall furnish an up-to-date, signed personal history statement and signed releases as necessary. In all cases, the reinvestigation shall include, as a minimum, appropriate National agency checks, local agency checks, (including overseas checks where appropriate), credit checks and a personal discussion interview with the individual by trained investigative, security or counterintelligence personnel when necessary to resolve significant adverse information and/or inconsistencies. When conditions so indicate, additional investigation may be conducted as determined by the SIO or his designee.

*In DoD, an SIO may request, with the appropriate of the Secretary of Defense, or his designee, more frequent investigations under special circumstances.

37 Determination of Access Eligibility

15. The evaluation of the information developed by investigation on an individual's loyalty and suitability shall be accomplished under the cognizance of the SIO concerned by analysts of broad knowledge, good judgment and wide experience in personnel security and/or counterintelligence. When all other information developed on an individual is favorable, a minor investigative requirement which has not been met should not preclude favorable adjudication. In all evaluations the protection of the National interest is paramount. Any doubt concerning personnel having access to SCI shall be resolved in favor of the National security. The ultimate determination of whether the granting of access is clearly consistent with the interest of National security shall be an overall common sense determination based on all available information.

38 Appeals Procedures

16. Annex B prescribes common appeals procedures to be followed when an individual's SCI access has been denied or revoked.

Continuing Security Programs

39 17.~~16~~ In order to facilitate the attainment of the highest standard of personnel security and to augment both the access approval criteria and the investigative requirements established by this Directive, member departments and agencies shall institute continuing security programs for all individuals having access to SCI. In addition to security indoctrinations, (See Annex ~~D~~C, "Minimum Standards for SCI Security Awareness Programs in the U.S. Intelligence Community"), these programs shall be tailored to create mutually supporting procedures under which no issue will escape notice or be left unresolved which brings into question an individual's loyalty and integrity or suggests the possibility of his being subject to undue influence or duress through foreign relationships or exploitable personal conduct. When an individual is assigned to perform sensitive compartmented work requiring access to SCI, the SIO for the department, agency, or Government program to which the individual is assigned shall assume security supervision of that individual throughout the period of his assignment.

18.~~17~~ The continuing security programs shall include the following:

a. SCI Security education programs ~~to ensure that individuals who are granted access to SCI are initially indoctrinated and periodically thereafter instructed as to the unique sensitivity and that they understand their personal responsibility for maintaining eligibility for continued access to SCI rests with the individual.~~ of the member departments and agencies shall be established and maintained pursuant to the requirements of Annex ~~D~~C. Additionally, ~~Therefore~~, the individual is encouraged to seek appropriate guidance and assistance on any personal problem or situation which may have a possible bearing on his eligibility for continued access to SCI, and security counseling should be made available. These instructions should be conducted by individuals having extensive background and experience regarding the nature and special vulnerabilities of the particular type of compartmented information involved.

b. Security supervisory programs to ensure that supervisory personnel recognize and discharge their special responsibility in matters pertaining to the security of SCI, including the eligibility for SCI access. Such programs shall provide practical guidance as to indicators which may signal matters of security concern. Specific instructions concerning reporting procedures shall be disseminated to enable the appropriate authority to take timely corrective action to safeguard the security of the United States as well as to provide all necessary help to the individual concerned to neutralize his vulnerability.

c. Security Review Programs to ensure that appropriate security authorities invariably receive and exchange, in a timely manner, all information bearing on the security posture of persons having access to sensitive information. Personnel history information shall be kept current. Security and related files shall be kept under continuing review.

19.18 Whenever adverse or derogatory information is discovered or inconsistencies arise which could impact upon an individual's security status, appropriate investigations shall be conducted on a timely basis. The investigation shall be of sufficient scope necessary to resolve the specific adverse or derogatory information, or inconsistency, in question so that a determination can be made as to whether the individual's continued utilization in activities requiring SCI is clearly consistent with the interests of the National security.

Effective Date

(40) 20.18 This Directive supersedes DCID 1/14, 1 JULY 1988, 13 May 1976. Existing directives,[4] regulations, agreements and such other references governing access to SCI as defined herein shall be revised accordingly.

---

[4]These include pertinent provisions of the Clearance Standards and Investigation and Evaluation section of the ~~Communications~~ Signals Intelligence Security Regulations.

(41)

(42)

WILLIAM J. CASEY

~~GEORGE BUSH~~
Director of Central Intelligence

19 March 1980

ANNEX A

DCID 1/14 ADJUDICATION GUIDELINES

PURPOSE

This annex is designed to ensure that a common approach is followed by Intelligence Community Departments and Agencies in applying the standards of DCID 1/14. These guidelines apply to the adjudication of cases involving persons being considered for first time access to Sensitive Compartmented Information (SCI) as well as those cases of persons being readjudicated for continued SCI access.

ADJUDICATIVE PROCESS

The adjudicative process entails the examination of a sufficient period of a person's life to make a determination that the person is not now or is not likely to later become an unacceptable security risk. SCI access adjudication is the careful weighing of a number of variables known as the "whole person" concept. The recency of occurrence of any adverse incident, together with circumstances pertaining thereto, is central to a fair and uniform evaluation. Key factors to be considered in adjudication are the maturity and responsibility of the person at the time certain acts or violations were committed as well as any repetition or continuation of such conduct. Each case must be judged on its own merits and final determination remains the responsibility of the individual SIO. Any doubt concerning personnel having access to SCI shall be resolved in favor of the national security.

The ultimate determination of whether the granting of SCI access is clearly consistent with the interests of national security shall be an overall common sense determination based on all available information. In arriving at a decision consistent with the foregoing, the adjudicator must give careful scrutiny to the following matters:

a. Loyalty
b. Close relatives and associates
c. Homosexual conduct and sexual perversion
d. Cohabitation
e. Undesirable character traits
f. Financial irresponsibility
g. Alcohol abuse
h. Illegal drugs and drug abuse
i. Emotional and mental disorders
j. Record of law violations
k. Security violations

Adjudicative actions concerning the foregoing items are examined in greater detail below.

LOYALTY

DCID 1/14 establishes the categorical requirement that, to be eligible for SCI access, an individual must be of unquestioned loyalty to the United States.

MISSING PAGE

ORIGINAL DOCUMENT MISSING PAGE(S):

page #9

Approved For Release 2006/01/03 : CIA-RDP87B01034R000500140077-2

COHABITATION

(43) Cohabitation with a member of the opposite sex in and of itself does not preclude SCI access approval.

The identity of a cohabitant must be ascertained and a determination made if such association constitutes an unacceptable security risk based on the same criteria as in the section dealing with Close Relatives and Associates. Cohabitation with an alien, for example, requires the same scrutiny as marriage to an alien. Extra-marital sexual relations are also of legitimate concern to the SCI adjudicator when the potential for undue influence or duress exists.

UNDESIRABLE CHARACTER TRAITS

It is emphasized that an individual's lifestyle is examined only in an effort to determine whether a pattern of behavior exists which indicates that granting SCI access could pose a risk to national security. In cases where allegations have been reported which reflect unfavorably on the reputation of an individual, it is incumbent upon the SCI adjudicator to distinguish fact from opinion and to determine which negative characteristics are real and pertinent to an evaluation of the individual's character and which are unsubstantiated or irrelevant. Relevant negative characteristics are those which, in the adjudicator's informed opinion, indicate that an individual is not willing, able, or likely to protect SCI information. The adjudicator's personal likes or dislikes must not be permitted to affect the determination.

(44) Examples of specific concern in determining whether an individual has undesirable character traits are any substantive credible derogatory comments by associates, employers, neighbors and other acquaintances; any litigation instituted against the individual by such persons as a result of the individual's actions; or allegations of violations of law. A recommendation for disapproval would be appropriate for an individual who cannot be relied upon to obey rules and regulations.

MISSING PAGE

ORIGINAL DOCUMENT MISSING PAGE(S):

pages 11, 12, 13, 14, 15, 16

Approved For Release 2006/01/03 : CIA-RDP87B01034R000500140077-2

MINIMUM STANDARDS FOR SCI SECURITY AWARENESS PROGRAMS IN THE U.S. INTELLIGENCE COMMUNITY

Minimum standards are hereby established for the SCI security education programs designed to enhance the security awareness of U.S. Government employees and private contractors working in the U.S. Intelligence Community. Compliance with these standards is required for all Departments/Agencies within the Intelligence Community. It is intended that existing security awareness programs shall be modified to conform with these standards. Departments/Agencies will establish a documented program, to ensure that training has been presented to all personnel.

The security awareness requirements set forth herein are divided into three phases. Phase I concerns the initial indoctrination of the employee which is normally administered prior to access to SCI ~~classified information~~. Phase II concerns the continuing security awareness program required to maintain and increase security awareness throughout the period of access. Phase III sets forth the final guidelines and instructions when access to SCI ~~classified information~~ is terminated.

I. Initial Indoctrination--As soon as practicable after being approved for access to SCI ~~classified information~~, employees shall receive an initial security indoctrination which shall include:

A. The need for and purpose of SCI ~~classified information~~, and the adverse effects to the national security that could result from unauthorized disclosure.

B. The intelligence mission of the Department/Agency to include the reasons why intelligence information is sensitive.

C. The administrative, personnel, physical and other procedural security requirements of the Department/Agency, and those requirements peculiar to specific duty assignments.

D. Individual classification management responsibilities as set forth in appropriate directives and regulations to include classification/declassification guidelines and marking requirements.

E. The definitions and criminal penalties for espionage, including harboring or concealing persons; gathering, transmitting, or losing defense information; gathering or delivering defense information to aid foreign governments; photographing and sketching defense installations; unauthorized disclosure of classified information (Title 18, U.S.C., Sections 792 through 795, 797 and 798), the Internal Security Act of 1950 (Title 50, U.S.C., Section 783) and, when appropriate, the Atomic Energy Act, Sections 224 through 227.

F. The administrative sanctions for violation or disregard of security procedures.

G. A review of the techniques employed by foreign intelligence organizations in attempting to obtain national security information.

H. Individual security responsibilities including:

1. The prohibition against discussing SCI ~~classified information~~ in a nonsecure area, over a nonsecure telephone or in any other manner that permits access by unauthorized persons.

2. The need to determine, prior to disseminating SCI ~~classified information~~, that the prospective recipient has the proper security access approval ~~clearance~~, that the ~~classified information~~ SCI is needed in order to perform official duties and that the recipient can properly protect the information.

3. Administrative reporting requirements such as foreign travel, contacts with foreign nationals, attempts by unauthorized individuals to obtain national security information, physical security deficiencies and loss or possible compromise of ~~classified~~ SCI material.

4. Obligation to report to proper authorities any information which could reflect on the trustworthiness of an individual who has access to SCI classified-information, such as:

a. Willful violation of security regulations

b. Unexplained affluence or excessive indebtedness

c. Serious unlawful acts

d. Apparent mental or emotional problems

e. Coercion or harassment attempts

f. Blackmail attempts

5. Identification of the elements in the Department/Agency to which matters of security interest are to be referred.

II. Periodic Employee Awareness Enhancement--Each Department/Agency shall establish a continuing security awareness program which will provide for frequent exposure of personnel to viable security awareness material. Implementation of a continuing program may include live briefings, audio-visual presentations (e.g., video tapes, films and slide/tape programs), printed material (e.g., posters, memoranda, pamphlets, fliers) or a combination thereof. It is essential that current information and materials are utilized. Programs should be designed to meet the individual needs of the Department/Agency.

A. The basic elements for this program shall include, but are not limited to, the following:

1. The foreign intelligence threat.

2. The technical threat.

3. Administrative, personnel, physical and procedural security.

4. Individual classification management responsibility.

5. Criminal penalties and administrative sanctions.

6. Individual security responsibilities.

7. A review of other appropriate Department/Agency requirements.

B. Special security briefings/debriefings are required to supplement the existing security awareness programs in the following situations:

1. When an employee is designated as a courier.

2. When an employee travels, officially or unofficially, to or through communist countries, or areas of high risk.

3. When an employee has, or anticipates, contact with representatives of communist controlled countries.

4. When an employee is granted access to SCI ~~sensitive-compartmented-information~~ or cryptographic material.

5. When any other situation arises for which a special briefing/debriefing is required by the Department/Agency.

III. Debriefing--When a Department/Agency has determined that access to SCI ~~classified-information~~ is no longer required, final instructions and guidelines will be provided to the employee. As a minimum these shall include:

A. A requirement that the individual read appropriate section of Titles 18 and 50, U.S. Code, and that the intent and criminal sanctions of these laws relative to espionage and unauthorized disclosure be clarified.

B. The continuing obligation never to divulge, publish, or reveal by writing, word, conduct or otherwise, to any unauthorized persons any SCI ~~classified-information-relating-to-the national-security~~, without the written consent of appropriate Department/Agency officials.

C. An acknowledgement that the individual will report without delay to the Federal Bureau of Investigation, or the Department/Agency, any attempt by an unauthorized person to solicit national security information.

D. A declaration that the individual no longer possesses any documents or material containing SCI ~~classified-information~~.

E. A reminder of the risks associated with foreign travel and certain hazardous activities as defined in DCID 1/20, and Department/Agency reporting requirements as applicable.