



ENCLOSURE 1

DoD Directive 5210.45

3-14
e



May 9, 1964
NUMBER 5210.45

Department of Defense Directive

SUBJECT Personnel Security in the National Security Agency

Reference (a) Public Law 88-290, An Act to Amend the Internal Security Act of 1950

I. PURPOSE

The purpose of this directive is to prescribe policies and procedures to implement Public Law 88-290, the objective of which is to strengthen personnel security in the National Security Agency.

II. PERSONNEL SECURITY STANDARD

No person shall be employed in, or detailed or assigned to, the National Security Agency, and no person shall have access to classified information of the Agency, unless his employment, detail, or assignment to the Agency, or his access to classified information of the Agency, is clearly consistent with the national security.

III. FULL FIELD INVESTIGATION

A. No person shall be finally employed in the National Security Agency until he has been the subject of a full field investigation. A person may, however, be
X provisionally employed before the completion of a full field investigation in his case, but he may not be given access to sensitive cryptologic information while he is so employed. His provisional employment is conditional upon the successful outcome of a full field investigation in his case.

B. No person shall be assigned or detailed to the Agency without the agreement of the Agency that its security requirements are met; each such person shall be the subject of a full field investigation.

in connection with such assignment or detail unless he has a current security clearance for sensitive cryptologic information which was granted under the same or equivalent standards as are prescribed by the Agency.

- C. The Director of the Agency may, in an exceptional case, temporarily waive the requirement for a full field investigation if he personally determines in writing that such action is advisable in the national interest and is clearly consistent with the national security. In such a case priority shall be given to the full field investigation. This authority of the Director, NSA, cannot be redelegated.

IV. BOARDS OF APPRAISAL

- A. The Director of the Agency shall establish one or more boards of appraisal of three members each to be assigned personnel security responsibilities as set forth below. Members of a board shall be senior officials with broad experience, shall be specially trained for their duties, and shall have been the subject of a full field investigation, and have been cleared for access to classified information, in connection with their appointment.
- B. The Director of the Agency shall refer to a board those cases in which he determines that there is a doubt as to eligibility for access to classified information of an employee or person assigned or detailed to the Agency. The board shall appraise the loyalty and suitability of persons whose cases have been referred to it and advise the Director whether access to classified information by such persons is clearly consistent with the national security. In applying the foregoing standard, the board shall use the criteria which have been prescribed by the U. S. Intelligence Board and Department of Defense Directive 5210.8 dated February 15, 1962.
- C. Proceedings of a board shall not include notice to the individual, right to a hearing, or appeal from an adverse recommendation. A board shall submit to the Director a report and recommendation on each case referred to it. The report shall not be made available to the person. No person shall be cleared for access or continued access to Agency classified information contrary to the recommendation of

May 9, 64

5210.45

a board except on the authority of the Director or, upon the referral by the Director, of the Secretary of Defense. In such a case, the Director or the Secretary shall make a determination in writing that the employment, detail, assignment or access is in the national interest.

- D. Appraisal by a board is not required before action may be taken under Section 14 of the Act of June 27, 1944, Chapter 287, as amended (5 U.S.C. 863), Section 1 of the Act of August 26, 1950, Chapter 803, as amended (5 U.S.C. 22-1), or any other similar provision of law. The objective in establishing the boards(s) is to assure further that the access of each person to classified information is clearly consistent with the national security in consonance with the requirements and standards of the U. S. Intelligence Board and the Department of Defense.

V. TERMINATION OF EMPLOYMENT

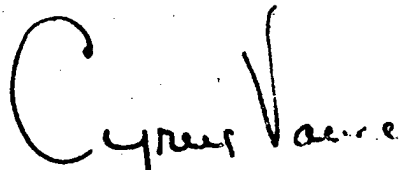
- A. Section 303 (a) of Public Law 88-290 authorizes the Secretary of Defense to terminate employment of any officer or employee of the National Security Agency in his discretion whenever (1) he considers such action to be in the interest of the United States, and (2) he determines that the procedures prescribed in other provisions of law that authorize the termination of employment of that officer or employee cannot be invoked consistently with the national security. The Secretary's action to terminate employment is final. The statute provides, however, that the individual whose employment has been terminated under this authority may seek or accept employment in any other Government agency provided that the Civil Service Commission determines he is eligible for such employment.
- B. When the two conditions cited above do not exist, the Director, NSA, shall, when appropriate, take action pursuant to other provisions of law, as applicable, to terminate the employment of a civilian officer or employee. The Director shall recommend to the Secretary of Defense the exercise of the authority of Section 303 (a) only when the termination of the employment of a civilian officer or employee cannot, because of paramount national security interests, be carried out under any other provision of law.

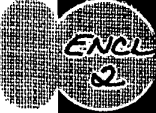
VI. IMPLEMENTATION

Proposed implementing regulations of the National Security Agency shall be coordinated with the General Counsel of the Department of Defense prior to their publication.

VII. EFFECTIVE DATE

This directive becomes effective immediately.


Deputy Secretary of Defense



ENCLOSURE 2

DCID 1/14

27 Nov 1987



**Director of
Central
Intelligence**

S-4
/3

Director of Central Intelligence Directive No. 1/14

**Minimum Personnel Security
Standards and Procedures
Governing Eligibility
for Access to
Sensitive Compartmented
Information**

27 November 1987

DIRECTOR OF CENTRAL INTELLIGENCE
DIRECTIVE NO. 1/14

(Effective 14 April 1986)

DIRECTOR OF CENTRAL INTELLIGENCE DIRECTIVE 1/14¹

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

(Effective 14 April 1986)

Pursuant to the provisions of Section 102 of the National Security Act of 1947, and Executive Order 12333, 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 (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.

1. *Definitions*

- a. *Intelligence Community*—those United States Government organizations and activities identified in Executive Order 12333 or successor orders as making up such Community.
- b. *Sensitive Compartmented Information (SCI)*—is classified information concerning or derived from intelligence sources, methods, or analytical processes that is required to be handled exclusively within formal access control systems established by the Director of Central Intelligence.
- c. *Senior Officials of the Intelligence Community (SOICs)*—for the purposes of this directive, SOICs are defined as the heads of organizations within the Intelligence Community, as defined by Executive Order 12333, or their designated representatives.

2. *Purpose*

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.

3. *Applicability*

The provisions of this 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.

4. *General*

- a. 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

¹ This directive supersedes DCID 1/14, effective 27 November 1984.

ineligible for access to other classified information. Individuals whose access to SCI has been authorized as an exception granted in accordance with paragraph 6 below, shall not, solely for that reason, be considered eligible for access to other classified information.

- b. The granting of access to SCI shall be controlled under the strictest application of the "need-to-know" principle, and in accordance with the personnel security standards and procedures set forth in this directive. In accordance with National Security Decision Directive Number 84 and the DCI Security Policy Manual for SCI Control Systems, signature of a DCI-authorized Nondisclosure Agreement which includes a provision for ~~prepublication review~~ is a condition of access to SCI.

5. Personnel Security Standards

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

- a. The individual shall be stable; trustworthy; reliable; of excellent character, judgment, and discretion; and of unquestioned loyalty to the United States.
- b. Except where there is a compelling need, and a determination has been made by competent authority as described in paragraph 6 below that every reasonable assurance has been obtained that under the circumstances the security risk is negligible:
 - (1) Both the individual and the members of his or her immediate family shall be U.S. citizens. For these purposes, "immediate family" includes the individual's spouse, parents, brothers, sisters, and children.¹
 - (2) The members of the individual's immediate family and persons to whom he or she is bound by affection or obligation² 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.

6. Exceptions to Personnel Security Standards

The exceptions to paragraph 5.b.(1) or (2) above may be granted only by the SOIC of the appropriate 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 organization making the exception. In those cases in which the individual has lived outside of the United States for a substantial period of his or her 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.

7. Investigative Requirements

- a. 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.

¹ The requirement for U.S. citizenship in this DCID also applies to a cohabitant.

² Including a cohabitant.

- b. 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.
- c. 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.


8. 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 of the individual's residence, 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 or, if such checks are not productive, through interviews with knowledgeable sources covering all areas of employment, residence, and education in the most recent 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 coworkers at places of employment covering the past ten (10) years shall be accomplished.
- g. Verification of graduation or attendance at all institutions of higher learning within the past fifteen (15) years. If the individual did not attend an institution of higher learning, verification of graduation or attendance at last secondary school within the past ten (10) years.
- h. Review of appropriate military records.
- i. Interviews with a sufficient number of knowledgeable sources (a minimum of three developed during the course of the investigation) as necessary to provide continuity, to the extent practicable, of the individual's activities and behavioral patterns over the past fifteen (15) years.
- j. When employment, education, or residence has occurred in foreign countries (except for periods of less than 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 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 one year, the investigation will be expanded to cover fully this period in his or her 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.

- k. When the individual has immediate family members or other persons to whom 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 cohabitant 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 affection 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 (see Annex A).
- m. A personal interview of the individual may be conducted by trained security, investigative, or counterintelligence personnel to ensure full investigative coverage. A personal interview will be conducted when necessary to resolve any significant adverse information and/or inconsistencies developed during the investigation. In departments or agencies with policies sanctioning the use of the polygraph for personnel security purposes, ~~the personal interview may include a polygraph examination, conducted by a qualified polygraph examiner.~~

9. *Exceptions to Investigative Requirements*

- a. In exceptional cases, the SOIC 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 8 above.~~ In this situation, such investigative checks as are immediately possible shall be made at once and 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.
-  b. ~~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 8 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 information.~~

10. Periodic Reinvestigations

- a. 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 or her activities are otherwise suspect, or when deemed necessary by the SOIC concerned.
- b. ~~The scope of reinvestigations shall be determined by the SOIC 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 evaluate continually 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, overseas checks where appropriate, credit checks, and a personal 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 SOIC or his designee.~~

11. Outside Activities

Individuals who hold, or are being considered for, SCI access approval shall have made available to them for reading the second and third paragraphs of the "Outside Activities" section of Annex A to DCID 1/14, and shall be instructed to report in writing to their security officer any existing or contemplated outside employment or activity that appears to meet the criteria of those paragraphs. Written reports must be submitted before beginning any outside employment or activity as defined in Annex A to DCID 1/14. In addition, initial or updated personal history statements must include details of outside employment or activities (as defined in Annex A to DCID 1/14). Investigation must cover the reported outside employment or activities. Information concerning actual or planned outside employment or activities that would create a potential risk to the security of SCI shall be evaluated in accordance with the factors specified in Annex A to determine whether the circumstances create an unacceptable risk of unauthorized disclosure.

12. Determination of Access Eligibility

The evaluation of the information developed by investigation on an individual's loyalty and suitability shall be accomplished under the cognizance of the SOIC 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 should be resolved in favor of the national security and the access should be denied or revoked. ~~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.~~

13. Appeals Procedures

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

14. Continuing Security Programs

- a. In order to facilitate 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 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 or her being subject to undue influence or duress through foreign relationships or exploitable personal conduct. When an individual is assigned to perform sensitive work requiring access to SCI, the SOIC 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 or her assignment.

b. The continuing security programs shall include the following.

- (1) Individuals are required to inform the department or agency which granted their SCI access about any personal problem or situation which may have a possible bearing on their eligibility for continued access to SCI and to seek appropriate guidance and assistance. Security counseling should be made available. This counseling should be conducted by individuals having extensive background and experience regarding the nature and special vulnerabilities of the particular type of compartmented information involved.
- (2) SCI security education programs of the member departments and agencies shall be established and maintained pursuant to the requirements of Annex C.
- (3) Security supervisory programs shall be established and maintained to ensure that supervisory personnel recognize and discharge their special responsibility to safeguard SCI, including the need to assess continued eligibility for SCI access. These programs shall provide practical guidance on 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 or her vulnerability.
- (4) Security review programs to ensure that appropriate security authorities always receive and exchange, in a timely manner, all information bearing on the security posture of persons having access to SCI. Personal history information shall be kept current. Security and related files shall be kept under continuing review.

Whenever adverse or derogatory information is discovered or inconsistencies arise which could impact upon an individual's security status, appropriate investigation 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 interest of the national security.

15. Security Violations

Individuals determined to have disclosed classified information to any person not officially authorized to receive it may be considered ineligible for initial or continued SCI access. Determination will be based on an evaluation of all available information, including whether the disclosure was knowing, willful, negligent, or inadvertent. ~~A determination of ineligibility for individuals who currently hold SCI access shall result in immediate debriefing and termination of access for cause.~~

16. Implementation

Existing directives, regulations, agreements, and other guidance governing access to SCI as defined herein shall be revised accordingly.

William J. Casey
Director of Central Intelligence

ANNEX A

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 become an unacceptable security risk later. 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 SOIC. 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. Sexual considerations
- 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
- l. Involvement in outside activities

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.

CLOSE RELATIVES AND ASSOCIATES

DCID 1/14 requires close examination by the SCI adjudicator when members of an individual's immediate family and persons to whom he/she is bound by affection or obligation are not citizens of the United States, or their loyalty or affection is to a foreign power, or they are subject to any form of duress by a foreign power, or they advocate the violent overthrow or unconstitutional alteration of the Government of the United States.

Sharing living quarters with a person or persons, regardless of their citizenship status, may be indicative of a close relationship, whether or not it is considered intimate. The potential for adverse influence or for duress should be considered in any close or long-term relationship between the subject and another individual.

The adjudicator must assess carefully the degree of actual and potential influence that such persons may exercise on the individual based on an examination of the frequency and nature of personal contact and correspondence with and the political sophistication and general maturity of the individual.

A recommendation for access disapproval is appropriate if there is an indication that such relatives or associates are connected with any foreign intelligence service.

When there is a "compelling need" for SCI access for an individual whose family member is a non-U.S. citizen and the background investigation indicates that the security risk is negligible, an exception to paragraph 5.b.(1) or (2) of DCID 1/14 may be recommended.

In some circumstances, marriage of an individual holding SCI access approval could present an unacceptable security risk. Such individuals are required to file intent-to-marry statements. It is the responsibility of the SOIC to advise the individuals of the possible security consequences. If the individual marries a non-U.S. citizen, SCI access will be suspended until the case is readjudicated unless an appropriate investigation of the spouse, as required by Paragraph 8.l. of DCID 1/14, was conducted with favorable results. In readjudicating such cases, the same judgments and criteria as are reflected in this section apply.

SEXUAL CONSIDERATIONS

DCID 1/14 requires that, to be eligible for SCI access, individuals must be stable, of excellent character and discretion, and not subject to undue influence or duress through exploitable personal conduct.

Sexual promiscuity, prostitution, and extramarital relations are of legitimate concern to the SCI adjudicator where such conduct reflects a lack of judgment and discretion or when the conduct offers the potential for undue influence, duress or exploitation by a foreign intelligence service.

Deviant sexual behavior can be a relevant consideration in circumstances in which it indicates flawed judgment or a personality disorder, or could result in exposing the individual to direct or indirect pressure because of susceptibility to blackmail or coercion as a result of the deviant sexual behavior. Such behavior includes, but is not limited to, bestiality, fetishism, exhibitionism, necrophilia, nymphomania or satyriasis, masochism, sadism, pedophilia, transvestism, and voyeurism. Homosexual conduct is also to be considered as a factor in determining an individual's judgment, discretion, stability and susceptibility to undue influence or duress.

In examining cases involving sexual conduct of security significance, such as those described above, it is relevant to consider the age of the person, the voluntariness, and the frequency of such activities, the public nature and the recency of the conduct, as well as any other circumstances which may serve to aggravate or mitigate the nature or character of the conduct. A recommendation for disapproval is appropriate when, in view of all available evidence concerning the individual's history of sexual behavior, it appears that access to SCI could pose a risk to the national security.

COHABITATION

The identity of a cohabitant and the extent and nature of actual or potential influence upon the subject should be ascertained. Based upon the criteria in the section on Close Relatives

and Associates, a determination must be made whether such an association constitutes an unacceptable security risk.

Cohabitation, per se, does not preclude SCI access approval. Other factors could affect the access determination. Cohabitation with an alien, for example, requires the same scrutiny as marriage to an alien.

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.

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.

In examining the circumstances of cases involving incidents of untruthfulness, the adjudicator must weigh all factors with particular emphasis on establishing the intent of the individual. Where an individual has tried to obscure pertinent or significant facts by falsifying data, e.g., on the Personal History Statement by either omission or false entry, such action should be weighed heavily against recommending access. Failure to disclose derogatory personal information, such as a court martial or serious crime, would appear to be intentional and, consequently, would warrant a recommendation for disapproval.

FINANCIAL IRRESPONSIBILITY

Financial irresponsibility represents a serious concern to the SCI adjudicator. Persons who have engaged in espionage for monetary gain demonstrate the hazard of granting SCI access to an individual with overly expensive tastes and habits or living under the pressure of serious debt.

A recommendation for disapproval is appropriate when there is a pattern of financial irresponsibility and it appears that an individual has not made a conscientious effort to satisfy creditors. In such cases, the adjudicator should determine whether the individual had been notified about the debts and whether they were legally valid or ultimately satisfied.

When the financial irresponsibility alone is not of such magnitude to warrant disapproval, it may contribute to recommendation for denial of SCI access when there is other evidence of irresponsibility.

ALCOHOL ABUSE

The SCI adjudicator should examine any information developed relative to an individual's use of alcoholic beverages to determine the extent to which such use would adversely affect the ability of the individual to exercise the care, judgment, and discretion necessary to protect SCI information. The adjudicator should determine whether a pattern of impropriety exists, although one incident caused by alcohol abuse may be of such magnitude to warrant a recommendation for disapproval.

In determining the security impact of a person's pattern of alcohol use, the adjudicator should consider the circumstances, amount and rate of consumption, the time and place of consumption, and the physiological and behavioral effect such drinking has on the individual. For

example, does the individual's drinking result in absences from work or careless work habits? Does the individual become talkative, abusive, or manifest other undesirable characteristics? Does the individual drink until intoxicated? Has the individual been arrested for any acts resulting from the influence of alcohol?

In the absence of conclusive evidence, additional insight may be available from appropriate medical authorities. If the individual acknowledges having an alcohol abuse problem and is seeking help, it may be appropriate to defer access determination and monitor the individual's progress for a year or so.

If, after considering the nature and sources of the information, the adjudicator determines that an individual's drinking is not serious enough to warrant a recommendation for disapproval of SCI access, it may be appropriate to recommend approval with a warning at the time of indoctrination that future incidents of alcohol abuse may result in SCI denial. The adjudicator may also recommend a reinvestigation of the individual's use of alcohol after an appropriate period of time has passed.

ILLEGAL DRUGS AND DRUG ABUSE

The SCI adjudicator should examine all allegations of an individual's use, transport, transfer, sale, cultivation, processing and manufacturing of hallucinogens, narcotics, drugs and other materials and chemical compounds identified and listed in the Controlled Substance Act of 1970, as amended. Consequently, an individual's involvement in any of these activities is of direct concern to the SCI adjudicator in order to determine the individual's capability to exercise the care, discretion, and judgment required to protect SCI information. The use of these substances may lead to varying degrees of physical or psychological dependence as well as having a deleterious effect on an individual's mental state and ability to function.

Persons involved in drug trafficking, i.e., the commercial cultivation, processing, manufacturing, purchase, or sale of such substances should normally be recommended for disapproval.

In cases involving the use of drugs, the adjudicator must consider the nature of the substance used and whether the use is experimental or habitual. The frequency, recency, and circumstances surrounding said use are key elements. For example, has the individual used "hard" drugs or hallucinogens such as heroin, cocaine, or LSD? Has the individual used drugs regularly or only on occasion? Does the individual currently use drugs? Does the individual regularly purchase drugs or participate merely when offered drugs by others? Has the individual's behavior been affected by the use of drugs and, if so, to what extent?

Once the judgment is made that an individual is a habitual user of any controlled substance (multiple use beyond the point of mere experimentation), a recommendation for disapproval is appropriate. Moreover, even experimental use of hard drugs or hallucinogens, such as LSD, could warrant a recommendation for disapproval.

EMOTIONAL AND MENTAL DISORDERS

DCID 1/14 requires that persons considered for access to SCI be stable, trustworthy, reliable, and of excellent character, judgment and discretion. Emotional and mental disorders which interfere with an individual's perception of reality or reliability are of serious concern to the SCI adjudicator in determining whether an individual is able or willing to protect SCI information.

It is essential to obtain as much information as possible when an allegation has been made in this area. If feasible, the individual should be interviewed to obtain additional detail. When appropriate, government psychological and psychiatric personnel should be consulted so that psychiatric or psychological data may be properly evaluated.

If a current emotional instability appears to be a temporary condition (for example, caused by a death, illness, or marital breakup), it may be advisable to recommend postponing final action and rechecking the situation at a later date. This precludes a security disapproval for what may be a temporary condition which, when cured, would have no security implications.

Military and civilian personnel who decline to take medical/psychiatric tests when so directed by competent authority should not be recommended for SCI access.

RECORD OF LAW VIOLATIONS

In determining whether an individual is stable, trustworthy, and of excellent character, judgment, and discretion as required by DCID 1/14 for access to SCI, the adjudicator must weigh carefully any record of law violations by the individual. Although a pattern of repeated minor traffic violations could be significant, the adjudicator is principally concerned with more serious criminal violations or court actions reflecting adversely upon the individual's reliability or trustworthiness.

Each case involving convictions for criminal offenses must be considered from the standpoint of the nature and seriousness of the offense, the circumstances under which it occurred, how long ago it occurred, whether it was an isolated offense or a repeated violation of the law, the offender's age at the time, social conditions which may have a bearing on the individual's actions, and any evidence of rehabilitation.

Any conviction for a felony will normally support a recommendation for disapproval. If the offense was committed many years prior, the individual has shown evidence of rehabilitation, and the investigation shows no other derogatory information, an approval may be considered. A large number of minor offenses, however, could indicate irresponsibility and may support an adverse recommendation.

SECURITY VIOLATIONS

Most security violations are caused by carelessness or ignorance with no intention of compromising security. However, the record of an individual responsible for multiple violations should be scrutinized. The individual's current attitude toward security should be confirmed with his/her supervisor. A pattern of violations may be sufficient ground for a recommendation for disapproval. Individuals responsible for unauthorized disclosure of classified information may be denied initial or continued SCI access.

OUTSIDE ACTIVITIES

Involvement in non-US Government employment or activities that raise potential conflicts with an individual's responsibility to protect classified information is of security concern and must be evaluated by a security officer to determine whether the conflict is of such a nature that SCI access should be denied or revoked.

Employment that must be reported includes compensated or volunteer service with any foreign national, with a representative of any foreign interest, or with any foreign, domestic, or international organization or person engaged in analysis, discussion, or publication of material on intelligence, defense, or foreign affairs.

Activities that must be reported include association with nationals of Communist countries or countries hostile to the United States; membership in organizations which have as members nationals of Communist countries or countries hostile to the United States when the membership involves contact with those nationals; and sponsorship of the entry of aliens into the United States.

Adjudicators of new SCI access evaluations shall carefully consider whether an individual's outside employment or activities may pose a conflict with his or her security responsibilities that could result in his or her disclosing classified information to unauthorized

persons. Any doubt as to an individual's willingness or ability to safeguard classified information shall be resolved by denying SCI access.

Reports from individuals approved for SCI access or from other sources concerning outside employment or activities of security concern shall be evaluated by security officials to determine if SCI access should be continued. When an individual's outside employment or activity raises doubts as to individual's willingness or ability to safeguard classified information, he or she shall be advised that continuing that employment or activity may result in withdrawal of SCI access, and be given an opportunity to discontinue. If the individual terminates the outside employment or activity of security concern, his or her SCI access approval(s) may be continued, provided that this is otherwise consistent with national security requirements.

ANNEX B

APPEALS

POLICY

This annex establishes common appeals procedures for the denial or revocation of access to Sensitive Compartmented Information (SCI) by entities of the Intelligence Community after adjudication pursuant to the provisions of DCID 1/14. This annex is promulgated pursuant to Executive Order 12333, Executive Order 12356 and Section 102 of the National Security Act of 1947. For the purpose of this annex, all references to DCID 1/14 include the basic document and all of its annexes. Any person who has been considered for initial or continued access to SCI pursuant to the provisions of DCID 1/14 shall, to the extent provided below, be afforded an opportunity to appeal the denial or revocation of such access. This annex supersedes any and all other practices and procedures for the appeal of the denial or revocation of SCI access. This annex shall not be construed to require the disclosure of classified information or information concerning intelligence sources and methods, nor shall it be construed to afford an opportunity to appeal prior to the actual denial or revocation of SCI access. In addition, the provisions of DCID 1/14, this annex, or any other document or provision of law shall not be construed to create a property interest of any kind in the access of any person to SCI. Further, since the denial or revocation of access to SCI cannot by the terms of DCID 1/14 render a person ineligible for access to other classified information solely for that reason, the denial or revocation of SCI access pursuant to the provisions of DCID 1/14 and this annex shall not be construed to create a liberty interest of any kind.

APPLICABILITY

This annex applies to all United States Government civilian and military personnel, as well as any other individuals, including contractors and employees of contractors, who are considered for initial or continued access to SCI. This annex does not apply to decisions regarding employment and shall not be construed to affect or impair Public Law 88-290 or the authority of any entity to effect applicant or personnel actions pursuant to Public Law 88-290, Public Law 86-36, or other applicable law.

SCI ACCESS DETERMINATION AUTHORITY

Adjudications for access to SCI shall be made in accordance with DCID 1/14 by a Determination Authority designated by the Senior Official of the Intelligence Community (SOIC) of each entity. Access to SCI shall be denied or revoked whenever it is determined that a person does not meet the security standards provided for in DCID 1/14.

PROCEDURES

1. Persons shall be:
 - a. notified of the denial or revocation of SCI access;
 - b. notified that they may request to be provided the reasons for such denial or revocation; and/or
 - c. afforded an opportunity to appeal,

whenever the Determination Authority of any entity, in the exercise of his or her discretion, deems such action in any given case to be clearly consistent with the interests of the national security.

2. Any person who is given notification and afforded an opportunity to appeal pursuant to paragraph 1. above may, within 45 days of the date on which such person is notified of the reasons for denial or revocation of SCI access, submit a written appeal of that denial or revocation to the Determination Authority. The written material submitted for consideration may include any information which the person believes will assist the Determination Authority in reviewing the case.

3. After a further review of the case in the light of the written appeal, the person will be notified of the decision of the Determination Authority.

4. If the Determination Authority reaffirms a denial or revocation of access, the person may, within 30 days of the date on which such person is notified of the Determination Authority's reaffirmation, request a final review of the case. In that event, the SOIC, or his or her designee, shall personally review the case and exercise his or her discretion pursuant to the provisions of DCID 1/14, and shall inform the person of his or her decision, which shall be final and unreviewable.

ANNEX C

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 civilian and military personnel and private contractors working in the U.S. Intelligence Community. Compliance with these standards is required for all departments/agencies within the Intelligence Community. 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.

All individuals nominated for or holding SCI access approval shall be notified initially and annually thereafter of their responsibility to report to their cognizant security officers any outside employment or activities (described in DCID 1/14, Annex A) that could conflict with their duty to protect classified information from unauthorized disclosure. Any other outside employment or activities which could create real or apparent conflicts with their responsibility to protect classified information also must be reported. Individuals granted SCI access approvals shall be advised:

- whom they may consult to determine if particular outside employment or activity might be of security concern;
- of the need to exercise security caution in their activities as members of professional, commercial, scholarly, or advocacy organizations that publish or discuss information on intelligence, defense, or foreign affairs; and
- of their continuing obligation to submit for review any planned articles, books, speeches, or public statements that contain or purport to contain SCI or information relating to or derived from SCI, as specified by the nondisclosure agreements that are a prerequisite for access to SCI.

The security awareness requirements set forth herein are divided into three phases. Phase 1 concerns the initial indoctrination of individuals which is normally administered prior to access to SCI. Phase 2 concerns the continuing security awareness program required to maintain and increase security awareness throughout the period of access. Phase 3 sets forth the final guidelines and instructions when access to SCI is terminated.

1. Initial Indoctrination—As soon as practicable after being approved for access to SCI, personnel shall receive an initial security indoctrination which shall include:

- a. The need for and purpose of SCI, and the adverse effect on 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 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, that the prospective recipient has the proper security access approval, that the 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 persons to obtain national security information, physical security deficiencies, and loss or possible compromise of 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, 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, and or
 - (f) blackmail attempts.
 - (5) Identification of the elements in the department/agency to which matters of security interest are to be referred.

2. Periodic Awareness Enhancement—Each department/agency shall establish a continuing security awareness program which will provide for frequent exposure of personnel to 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 be utilized. Programs should be designed to meet the particular 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 individual is designated as a courier.
 - (2) When an individual travels, officially or unofficially, to or through Communist countries, or areas of high risk.
 - (3) When an individual has, or anticipates, contact with representatives of Communist-controlled countries.
 - (4) When any other situation arises for which a special briefing/debriefing is required by the department/agency.

3. Debriefing—When a department/agency has determined that access to SCI is no longer required, final instructions and guidelines will be provided to the individual. As a minimum these shall include:

- a. A requirement that the individual read appropriate sections 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, under the prepublication and other provisions of the nondisclosure agreement for SCI, never to divulge, publish, or reveal by writing, word, conduct or otherwise, to any unauthorized persons any SCI, 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.
- e. A reminder of the risks associated with foreign travel and certain hazardous activities as defined in DCI Directive 1/20, *Security Policy Concerning Travel and Assignment of Personnel with Access to Sensitive Compartmented Information*, and department/agency reporting requirements as applicable.

ENCL
3

ENCLOSURE 3

NSA/CSS Regulation 120-12

5-4
4

**NATIONAL SECURITY AGENCY
CENTRAL SECURITY SERVICE
FORT GEORGE G. MEADE, MARYLAND**

NSA/CSS REG. NO. 120-12*

DATE: 31 July 1986



NSA/CSS REGULATION

PERSONNEL SECURITY PROGRAM FOR CONTINUED ACCESS

	<u>SECTION</u>
REFERENCES	I
PURPOSE AND APPLICABILITY	II
DEFINITIONS	III
POLICY.	IV
PROCEDURES	V
IMPLEMENTATION	VI

SECTION I - REFERENCES

1. References:

a. DoD Directive 5210.45, Personnel Security in the National Security Agency, dated 9 May 1964, implements Public Law 88-290, Personnel Security Procedures in the National Security Agency, 78 Stat. 168 (codified at 50 U.S.C. §§ 831-835).

b. DoD Directive 5100.23, Administrative Arrangements for the National Security Agency, dated 17 May 1967.

c. NSA/CSS Regulation No. 122-3, Polygraph Examinations and Examiners, dated 6 April 1984, implements DoD Directive 5210.48, DoD Polygraph Program, dated 24 December 1984.

d. NSA/CSS Directive 10-30, Procedures Concerning Activities of NSA/CSS That Affect U.S. Persons, dated 21 March 1983, implements Executive Order 12333, United States Intelligence Activities, dated 4 December 1981.

OPI: M5 M509, 982-7885s)

* This Regulation supersedes NSA/CSS Regulation Number 120-12, dated 20 September 1978.

STAT

NSA/CSS REG. NO. 120-12

e. Executive Order 12356, National Security Information, dated 2 April 1982.

f. Public Law 86-36, National Security Agency Act of 1959, as amended (50 U.S.C. §§ 402 note).

g. Director of Central Intelligence Directive 1/14, Minimum Personnel Security Standards and Procedures Governing Eligibility for Access to Sensitive Compartmented Information, dated 14 April 1986.

h. NSA/CSS Regulation No. 120-4, Security Supervision, 30 December 1985.

i. National Security Agency Regulation No. 30-4, National Security Agency Boards of Appraisal, dated 22 June 1964.

j. NSA Circular No. 122-1, Personnel Security Policies and Procedures for Personnel of the Service Cryptologic Elements Assigned to Duty with the National Security Agency, dated 10 August 1984.

k. Deputy Under Secretary of Defense for Policy memorandum, Polygraph Examination of Military Personnel Assigned/Detailed to NSA, dated 30 August 1984.

l. National Security Decision Directive 196, Counterintelligence/Countermeasure Implementation Task Force, dated 1 November 1985.

SECTION II - PURPOSE AND APPLICABILITY

2. This Regulation establishes programs within the National Security Agency/Central Security Service (NSA/CSS) to ensure that the ~~continued access of NSA/CSS personnel to~~ Protected Information is clearly consistent with the national security and to implement the access approval criteria and the investigative requirements established by the Director, NSA/CSS, the Director of Central Intelligence and the Secretary of Defense.

3. This Regulation is applicable to all NSA/CSS personnel. Visitors, second-party foreign liaison officers, and those persons detailed to the NSA/CSS for operational training are not considered NSA/CSS personnel.

SECTION III - DEFINITIONS

4. For purposes of this Regulation, the following definitions apply:

NSA/CSS REG. NO. 120-12

a. NSA/CSS Personnel: All persons employed by, assigned or detailed to the NSA/CSS, or any other individuals having access to NSA/CSS information and spaces. Visitors, second-party foreign liaison officers, and those persons detailed to the NSA/CSS for special operational training are exempt from this regulation.

b. Protected Information: Any information in one or both of the following categories which was obtained as a result of a relationship with NSA:

(1) Classified Information: All information classified or classifiable pursuant to the standards of Executive Order 12356, or any successor order, and implementing regulations. It includes, but is not limited to, intelligence and intelligence-related information, sensitive compartmented information (information concerning or derived from intelligence sources and methods), and cryptologic information (information concerning communications security and signals intelligence).

(2) Unclassified Sensitive Information: All information relating to the organization, functions, activities, and personnel of the NSA in accordance with Public Law 86-36. It includes, but is not limited to, the names, titles, salaries, and numbers of persons employed by, detailed or assigned to the NSA and to communications security information involving codes, ciphers, and cryptographic systems used by the United States Government or any foreign governments.

c. Satisfactory Completion of the Polygraph: The information contained in the polygraph examination report is favorably evaluated by security personnel, as described in paragraph 7, below, according to Director of Central Intelligence Directive 1/14 clearance criteria.

SECTION IV - POLICY

5. The continued access to NSA/CSS Protected Information and spaces by NSA/CSS personnel must be clearly consistent with the national security. The programs detailed in Section V have been established to ensure that this standard is met.

6. All NSA/CSS personnel are subject to the programs specified in Section V. Exceptions may be granted by the Office of Security for compelling operational reasons on a case-by-case basis. The information obtained shall serve as a major factor in determining eligibility for continued access to NSA/CSS Protected Information.

NSA/CSS REG. NO. 120-12

7. Evaluation of the investigative information will be conducted in accordance with Director of Central Intelligence Directive 1/14 clearance criteria by trained security personnel possessing mature judgment, and broad knowledge and experience in the security career fields. ~~The ultimate determination of whether to grant continued access to NSA/CSS Protected Information shall be an overall common sense determination based on all available information.~~ Any doubt concerning an NSA/CSS person's continued access to NSA/CSS Protected Information shall be resolved in favor of the national security.

8. Refusal to consent to, or unsatisfactory completion of any aspect of the programs listed in Section V, when established as a requirement for continued access, may result in adverse action, denial of continued access to NSA/CSS Protected Information and spaces, and/or termination of employment.

9. NSA/CSS personnel may not normally be granted additional special access, or a TDY or PCS assignment unless the individual's special background investigation or reinvestigation, as specified in paragraph 11, below, is current within five years, or unless a reinvestigation has at least been initiated.

SECTION V - PROCEDURES

10. Prior to the conduct of a personal interview or a polygraph examination, NSA/CSS personnel shall be provided and asked to sign an ~~interview consent form~~.

11. All NSA/CSS employees and contractor personnel with access to NSA/CSS Protected Information shall be included in the Reinvestigation Program (RIP). The RIP shall be conducted on a recurrent basis within a period not to exceed five years from the initial special background investigation or from the last reinvestigation. The RIP consists of the following procedures:

a. ~~Personal History forms~~ will be updated and used to initiate the RIP. As part of this process, supervisors will evaluate their subordinates relative to certain personnel security criteria (reference h.).

b. ~~A personal interview~~ will address topics to include foreign assignments/connections/associations, approaches by foreign intelligence, unreported breaches of

NSA/CSS REG. NO. 120-12

security procedures, and related suitability matters which have security impact such as drug usage, criminal activities or other matters set forth in Reference g. The interview will also include a review of the individual's updated Personal History forms. An opportunity will be afforded the individual to raise issues of security concern or make suggestions to improve the security program.

c. ~~At a minimum, investigative field work will include local police checks, credit bureau checks, national agency checks, and expanded investigation as necessary.~~

d. Individuals must satisfactorily complete a reinvestigation polygraph examination (RPG) which will consist of counterintelligence scope questions covering the following topics:

- (1) Involvement in espionage, sabotage or terrorist activity against the United States;
- (2) Knowledge of others involved in espionage, sabotage or terrorist activity against the United States;
- (3) Involvement in giving or selling classified material to unauthorized persons;
- (4) Knowledge of others giving or selling classified material to unauthorized persons; and
- (5) Unauthorized contact with representatives of a foreign government.

In the event of an incomplete or unsatisfactory polygraph examination, the individual will be rescheduled as soon as possible.

e. Assessment of information pertinent to an individual's continued access to NSA/CSS Protected Information will be accomplished in accordance with the provisions of paragraph 7, above. ~~Should that assessment indicate doubt that continued access is clearly consistent with the national security, the information will be forwarded, as appropriate, to the Deputy Director for Administration, NSA/CSS, who shall determine whether the case merits personnel action, temporary suspension of access, recommendation to the Director for removal of access, or referral to a Board of Appraisal.~~ ✓

f. Satisfactory completion of the RIP is necessary for continued access to NSA/CSS Protected Information.

NSA/CSS REG. NO. 120-12

12. Military personnel who possess a TOP SECRET Special Intelligence (TSSI) clearance granted by their parent military organization and who are nominated for assignment to the NSA/CSS will be subject to the following procedures:

a. All military persons will be administered a ~~military-entrance-polygraph-(MEP)-examination~~ consisting of ~~counterintelligence-scope-questions~~, by, or initiated by, their parent military organization. The military organization will evaluate the polygraph results and only those persons who satisfactorily complete the MEP will be assigned to the NSA/CSS. Any military individuals who report to the NSA/CSS who have not yet completed a MEP must show evidence of a scheduled polygraph.

b. Properly cleared and indoctrinated military personnel assigned to the NSA/CSS will receive a security orientation briefing and be scheduled for a personal interview through the Military Interview Program (MIP).

c. The MIP will address topics to include foreign assignments/connections/associations, approaches by foreign intelligence, unreported breaches of security procedures and related suitability matters which have security impact, such as drug usage and criminal activities.

d. Assessment of information pertinent to the military assignee's continued access to NSA/CSS Protected Information will be accomplished in accordance with the provisions of paragraph 7, above. Should that assessment indicate doubt that continued access is clearly consistent with the national security, appropriate action will be taken by Chief, M5, and may ultimately include forwarding the information to the Deputy Director for Administration, NSA/CSS, who shall determine whether the case merits action to limit, suspend, or terminate access to Agency facilities, or referral to the Director or the Board of Appraisal. The individual's parent military organization will be promptly informed of all such actions. Pursuant to the provisions of Reference j., appropriate military authorities will be advised of all actions which may impact upon the continued assignment or detail of military personnel to the NSA/CSS.

e. Satisfactory completion of the MEP and the MIP is necessary for continued access to NSA/CSS Protected Information. Satisfactory completion of the MIP is necessary before the military assignee will be eligible for additional accesses.

NSA/CSS REG. NO. 120-12

13. All NSA/CSS personnel are eligible for selection for the Aperiodic Polygraph (APG) Program at any time after their initial access. The APG consists of the following procedures:

a. Individuals will be randomly selected for the APG with attention given to appropriate security considerations such as sensitivity of access.

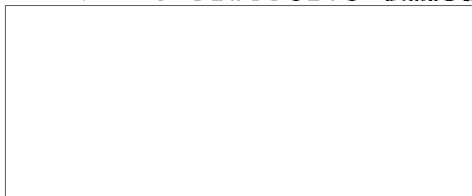
b. The polygraph examination will consist of relevant counterintelligence scope questions, as indicated in paragraph 11.d., above.

c. Assessment of the polygraph information shall be accomplished in accordance with the provisions of paragraph 7, above. Satisfactory completion of the APG examination is necessary to retain continued access at NSA/CSS.

14. Various sensitive programs and assignments at NSA/CSS have been designated by the responsible Office of Primary Interest (OPI) as requiring a Sensitive Access Examination (SAE) prior to selection for the program or assignment. The SAE is a polygraph examination consisting of counter-intelligence scope questions, as indicated in paragraph 11.d, above. Satisfactory completion of the SAE is necessary to obtain access to a program, project or assignment so designated.

SECTION VI - IMPLEMENTATION

15. This NSA/CSS Regulation is effective immediately.



Deputy Director
for
Administration

DISTRIBUTION II

Plus M509 (10 stock copies)
F92 (VRD)

ENC
4

ENCLOSURE 4

The Accuracy and Utility of Polygraph Testing

OOD
Wash DC
1984

Brown, paper back, $8\frac{1}{2} \times 11$ "

In pers security file as —

ENCLOSURE 5

Polygraph Utility Study



STAT

Page Denied

Next 14 Page(s) In Document Denied

