PDF Version

DCI Directive 6/4

Personnel Security Standards and Procedures Governing Eligibility for Access to Sensitive Compartmented Information (SCI)

DCID 1/14 was renumbered 6/4 by the Director of Central Intelligence (DC) and the Deputy Director of Central Intelligence for Community Management on 13 Oct 99, to more closely align the DCID with the new category structure as defined in DCID 1/1. This action was accomplished in conjunction with the DCI approving the newly created Annex F, "Reciprocity of SCI Eligibility Determinations."

This directive supersedes Director of Central Intelligence Directive 1/14, as amended 12 August 1994.

A complete copy of DCID 6/4 now consists of the basic DCID and Annexes A through F, as follows:

- Annex A - Investigative Standards for Background Investigations for Access to Classified Information.
- Annex B - Quality Control Guidelines for the Single Scope Background Investigation.

- Annex C - Adjudication Guidelines for Determining Eligibility for Access to Classified Information.
- Annex D - Appeals Procedures: Denial or Revocation of Access.
- Annex E - Standards for SCI Security Awareness Programs in the US Intelligence Community.
- Annex F - Reciprocity of SCI Eligibility Determinations (Annex F was created subsequent to the creation of the DCID. The DCI approved Annex F on 13 Oct 99.)

The President approved the Adjudicative Guidelines, Temporary Eligibility Standards and Investigative Standards required by Executive Order 12968 on March 24, 1997. This revised DCID incorporates the President's policy documents verbatim, at Annexes A and C, to promote the use of these common and consistent standards for government-wide security background investigations. These two annexes should be read in the context of the Director of Central Intelligence (DCI) special authorities, governing access eligibility to SCI, although the actual wording addresses a broader application to clearance actions.

The DCI exercises authority derived from statute and executive order over access eligibility to SCI and delegates this authority to Determination Authorities through Senior Officials of the Intelligence Community. (See Definitions.) Nothing in this directive or its annexes shall be deemed to preclude the DCI or the DDCI under the authority of the National Security Act of 1947, as amended, from taking any actions regarding an individual's SCI access.

Pursuant to the provisions of the National Security Act of 1947, as amended, and Executive Orders 12333 and 12968, the following personnel security guidelines, procedures, standards, and continuing security programs are hereby established for all US Government civilian and military personnel, consultants, contractors, employees of contractors,

and other individuals who require access to SCI. Individual departments and agencies may establish such additional security steps as may be deemed necessary and appropriate to resolve issues and/or address employment standards unique to them to ensure that effective security is maintained.

1. Definitions.

a. Cohabitant--A person living in a spouse-like relationship with the individual requiring SCI information.

b. Compelling Need--A signed determination by a Senior Official of the Intelligence Community (SOIC) or his/her designee that the services of an individual are deemed essential to operation or mission accomplishment.

c. Risk Assessment--A written evaluation supporting the adjudicative process, especially when a significant exception to a Personnel Security Standard is being considered. This assessment should consist of an evaluation from security, counterintelligence, and other technical or management experts as appropriate, and should contrast the compelling national security benefit of an individual accessed to SCI with the risk.

d. Determination Authority --A designee of a SOIC with responsibility for decisions rendered with respect to SCI access eligibility or ineligibility.

e. Immediate Family --The spouse, parents, siblings, children, and cohabitant of the individual requiring SCI access.

f. Intelligence Community --Those US Government organizations and activities identified in the National Security Act of 1947, as amended, 50 USC 401a(4), EO 12333, or successor orders, as making up such a Community.

g. Senior Officials of the Intelligence Community (SOICs) -- The heads of organizations or activities within the Intelligence Community, as defined by the National Security Act of 1947, as amended, 50 USC 401a(4), and EO 12333.

h. Sensitive Compartmented Information --Classified information concerning or derived from intelligence sources, methods, or analytical processes requiring handling exclusively within formal access control systems established by the DCI.

2. Purpose.

The purpose of this directive is to enhance the security protection of SCI through the application of personnel security standards, procedures, and continuing security programs.

3. Applicability.

The provisions of this directive will apply to all persons (other than elected officials of the US Government, to include elected State Governors as may be required on an individual basis, Federal judges, and those individuals for whom the DCI makes a specific exception) without regard to a civilian or military status, form of employment, official rank or position, or length of service. This directive does not apply to situations involving the duly authorized disclosure of SCI to representatives of foreign governments and international organizations.

4. General.

a. The granting of access to SCI will 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.

b. In accordance with DCID 1/19, "Security Policy for Sensitive Compartmented Information," and its supplement, "DCID 1/19 Security Policy Manual," those approved for access to SCI are required to sign a DCI-authorized nondisclosure agreement that includes a provision for prepublication review as 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 as follows:

a. The individual requiring access to SCI must be a US citizen.

b. The individual's immediate family must also be US citizens.

c. Members of the individual's immediate family and any other 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 or by persons who may be or have been engaged in criminal activity, 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.

d. The individual must be stable; trustworthy; reliable; of excellent character, judgment, and discretion; and of unquestioned loyalty to the United States.

6. Exceptions to Personnel Security Standards.

Any exception to the Personnel Security Standards will be a common sense determination based on the fact that the available information supports a finding that the specific risk to

national security is manageable in the specific case for which the exception is granted. The organization determining that an exception is warranted will document their finding in the individual's security record. As appropriate, a risk assessment, normally directed by the Determination Authority, may be required to aid in the determination of the appropriateness of granting an exception to one of the Personnel Security Standards. If accomplished, this assessment should become a part of the individual's security record.

a. The DCI is the exclusive authority for granting an exception to the requirement that the Subject be a US citizen.

b. The affected SOIC or specified designee may grant exception to the standard requiring US citizenship for the family members of an individual proposed for SCI access, as well as the standard requiring individuals to which Subject is bound by affection or obligation be free of any form of duress.

c. Exceptions to the US citizenship requirement for individuals to be accessed to SCI and their immediate family members shall require certification of a compelling need. This exception should be based upon a specific national security requirement and a certification of compelling need.

7. Investigative Requirements and Standards.

a. The investigation conducted on an individual under consideration for access to SCI will conform to the requirements of a Single Scope Background Investigation (SSBI) as defined in Annex A, "Investigative Standards for Background Investigations for Access to Classified Information." Quality Control procedures relevant to investigations are defined in Annex B, "Quality Control Guidelines for the Single Scope Background Investigation."

b. When conditions indicate, investigation of immediate

family members will be conducted to the extent necessary to permit a determination by the adjudicating agency that the provisions of paragraph 5 of this directive are met.

c. Where a previous investigation has been conducted within the past five years that meets the standards of Annex A, it will serve as a basis for granting access approval except where there is substantial information indicating that the employee may not satisfy the adjudicative guidelines in Annex C. If a previous investigation does not meet the Annex A standards, if it is more than five years old, or if there is a break in SCI access of two years or more, a current investigation will 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 Annex A of this directive, paragraphs 6 and 10. The up-dating process may be limited to review of applicable records, starting with an updated SF-86, and involve reinvestigation only when it appears the person may no longer satisfy standards for access under this directive. Should new information be developed during the current investigation that bears unfavorably on the individual's activities covered by the previous investigation, the current inquiries will be expanded as necessary to develop full details of this information.

d. Programs will be instituted requiring the periodic reinvestigation (PR) of personnel provided access to SCI. These SSBI-PRs will be conducted in accordance with the procedures and scope contained in the section of Annex A defining the SSBI-PR. The SSBI-PR may be expanded as necessary to resolve outstanding issues.

e. Notwithstanding the status of an individual's background investigation, departments and agencies with policies sanctioning the use of the polygraph for personnel security purposes may require polygraph examinations when deemed necessary by the department or agency head to be in the

national security interest of the United States. Where they exist, such polygraph programs shall be characterized by unified training and certification as well as by coordination of scope, applicability and fairness issues to promote consistency, reciprocity and due process.

f. In those cases in which the individual has lived outside of the United States for a substantial period, a thorough assessment of the adequacy of the investigation in terms of fulfillment of the investigative requirements and judicious review of the information therein must be made before an exception is considered.

8. Temporary Eligibility for Access to SCI.

a. In exceptional cases, including national emergency situations and hostilities involving US personnel, the SOIC or his designee may determine that it is necessary or advisable in the national interest to authorize temporary access to SCI before completion of the SSBI. In this situation, the procedures contained in the Annex A section entitled "Investigative Standards for Temporary Eligibility for Access" will be complied with before temporary access is permitted. A personal interview of the individual by trained security, investigative, or counterintelligence personnel will be conducted wherever possible and practicable.

b. The SSBI and final evaluation will be completed at the earliest practicable moment unless an exception is granted by the DCI. Temporary eligibility for access is valid only at the agency granting it and other agencies which expressly agree to accept it and acknowledge understanding of its investigative basis. Therefore, certification to other organizations of individuals authorized temporary access will include explicit notification of the fact.

c. Temporary eligibility for access may be granted only to

SCI necessary for the individual to perform authorized functions. Therefore, indoctrination briefings will be modified to the basic information necessary to ensure protection of the SCI to which the individual will be exposed, and appropriate nondisclosure agreements signed.

9. Reporting Requirements.

Individuals who hold SCI access have special responsibilities and obligations to report to their cognizant security officer, in writing and when feasible in advance, activities, conduct or employment that could conflict with their ability to protect classified information from unauthorized disclosure or counterintelligence threats. A more detailed explanation and a listing of an individual's responsibilities and reporting requirements are contained in Annex E. In addition, initial and updated security documents (e.g. Statement of Personal History, Questionnaire for National Security Positions, Security Clearance Application) and security records shall include details of such employment, activities, associations and/or conduct to facilitate appropriate investigation and evaluation to determine whether the circumstances create an unacceptable risk to the security of SCI or of unauthorized disclosure. Annex C, Guideline L, "Outside Activities," summarizes the concern.

10. Determinations of Access Eligibility.

The evaluation of the information developed by investigation of an individual's loyalty and suitability will be accomplished by trained professional adjudicators under the cognizance of the SOIC concerned. When all other information developed on an individual is favorable, a minor investigative requirement that has not been met should not preclude a favorable access determination by an authorized adjudicative authority. In all evaluations, the protection of the national security 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 will be an overall common sense determination based on all available information. The adjudicative guidelines for determining eligibility for access to SCI are contained in Annex C.

11. Appeals Procedures.

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

12. Continuing Security Programs.

a. To facilitate attainment of appropriate standards 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 based on risk management principles for all individuals having access to SCI. In addition to security indoctrinations (see Annex E, "Standards for SCI Security Awareness Programs in the US Intelligence Community"), these programs will be tailored to create mutually supporting procedures to identify and resolve issues which bring into question an individual's loyalty and integrity or suggest the possibility of his or her being subject to undue influence or duress through foreign relationships or exploitable personal conduct. These programs should include the capacity for member departments and agencies to monitor the individual’s performance in a tailored program against the eligibility criteria and adjudicative standards when unresolved concerns are present. 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 will assume security supervision of that individual throughout the period of his or her assignment.

b. The continuing security programs will include the following:

(1) Individuals are required to inform the department or agency that grants their SCI access about any personal problem or situation that may have a possible bearing on their eligibility for continued access to SCI and to seek appropriate guidance and assistance. Security guidance should be provided by an official who understands both the eligibility issues involved, and the unique sensitivities of the specific SCI program being supported. As appropriate, tailored monitoring programs should be established to ensure that individuals actively resolve problems which have led to concern about their continued eligibility for access. An individual participating in a monitoring program with a particular department or agency does not meet the criteria for automatic reciprocal acceptance of SCI eligibility as established by Executive Order 12968. In these situations, each organization should make their own determination of eligibility.

(2) SCI security education programs of the member departments and agencies will be established and maintained pursuant to the requirements of Annex E of this directive.

(3) Security awareness programs for supervisory personnel will 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 will provide practical guidance on indicators that may

signal matters of security concern. Specific instructions concerning reporting procedures will 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 will ensure that appropriate security authorities always receive and exchange, in a timely manner, all information, including lead information, bearing on the security posture of persons having access to SCI. Personal history information will be kept current. Security and related files will be kept under continuing review.

(5) Where permitted by agency policy, security review programs may include the use of polygraph examinations conducted by a qualified polygraph examiner.

c. Whenever adverse or derogatory information is discovered or inconsistencies arise that could impact on an individual's security status, appropriate investigation will be conducted on a timely basis. The investigation will 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 national security.

13. Implementation.

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

George J. Tenet
Director of Central Intelligence

July 2, 1998
Date