Next 1 Page(s) In Document Denied

9. **Security Indoctrination and Education.**

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

b. Subsequent to signing the NdA, persons shall be fully indoctrinated on the aspects of the SCI to which they are authorized access and have a demonstrated need-to-know. All persons granted SCI access shall periodically be advised of their continuing security responsibilities and of security threats they may encounter. Annex C to DCID 1/14, "Minimum Standards for SCI Security Awareness Programs in the U.S. Intelligence Community," provides guidance.

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

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

PHYSICAL SECURITY

12. **Construction and Protection Standards.** All SCI must be stored within accredited SCIFs. Physical security standards for the construction and protection of such facilities are prescribed in DCID 1/21, *Physical Security Standards for Sensitive Compartmented Information Facilities*, effective 12 April 1984, or successor policy statements.

DCID 1/19

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

14. **Emergency Plans.** Each accredited SCIF shall establish and maintain an approved emergency plan. This may be part of an overall department, agency, or installation plan, so long as it satisfactorily addresses the considerations stated below. Emergency planning shall also take account of fire, natural disasters, entrance of emergency personnel (e.g., host country police and firemen) into an SCIF, and the physical protection of those working in such SCIFs.