DIRECTOR OF INTELLIGENCE DIRECTIVE NO. 1/20

SECURITY POLICY CONCERNING TRAVEL AND ASSIGNMENT OF PERSONNEL WITH ACCESS TO SENSITIVE COMPARTMENTED INFORMATION (SCI)[1] (U)

(Effective)

Pursuant to Section 102 of the National Security Act of 1947 and Executive Order 12333, minimum security policy is herewith established for assignment and travel of U.S. Government civilian and military personnel, government consultants and employees of government contractors who have, or who have had, access to SCI.

1. Purpose

This policy is based upon the need to protect SCI from possible compromise resulting from the capture, interrogation, exploitation, or entrapment of SCI-knowledgeable personnel by hostile nations or groups or as a result of terrorist actions.

2. Definitions

a. **Defensive Security Briefings**--formal advisories which alert traveling personnel to the potential for harassment, provocation, or entrapment. These briefings, based on actual experience when available, include information on courses of action helpful in mitigating adverse security and personal consequences, and advise of

---

[1] This directive supersedes the policy statement on Security Policy Concerning Travel and Assignment of Personnel with Access to Sensitive Compartmented Information (SCI), effective 8 April 1983.

passive and active measures which personnel should take to avoid becoming targets or inadvertent victims of terrorism.

b. **Hazardous Activities**--assignments or visits to, and travel through, countries listed in the attached Appendix. Hazardous activities also include assignment or travel in combat zones or other areas where hostilities are taking place, duties behind hostile lines, and duties or travel in isolated or exposed areas where individuals cannot reasonably be protected against hostile action or in areas or countries subject to substantial risk of terrorist acts. The use of vessels owned or controlled by a country listed in the attached Appendix is also included.

c. **Terrorism**--premeditated, politically motivated violence perpetrated against noncombatant targets by subnational groups or clandestine state agents.

d. **Risk of Capture Briefings**--advisories which alert personnel as to what may be expected in the way of attempts to force or trick them to divulge classified information if captured or detained and of suggested courses of action they should follow to avoid or limit such divulgence. These advisories include instructions/advice for advance preparation of innocuous, alternate explanations of duties and background.

e **Senior Officials of the Intelligence Community (SOICs)**--for the purpose 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.

f **Sensitive Compartmented Information (SCI)**--all information and materials requiring special Community controls indicating restricted handling within present and future Community intelligence collection programs and their end products. These special Community controls are formal systems of restricted access established to protect the sensitive aspects of sources, methods, and analytical procedures of foreign intelligence programs. The term does not include Restricted Data as defined in Section II, Public Law 585, Atomic Energy Act of 1954, as amended.

3. **Policy**

Persons granted access to information about the sensitive aspects of sources, methods, and analytical procedures of foreign intelligence incur a special security obligation and are to be alerted to the risks associated with travel to, through, or within, or with other activities involving, the countries listed in the attached Appendix and areas or countries subject to substantial risk of terrorism.

a. **Official Travel.** No person with access to SCI will be assigned or directed to participate in a hazardous activity, as defined herein, until he or she has been afforded a defensive security briefing and/or risk of capture briefing by an official specified by the cognizant SOIC. (Consideration will be given to the relative protection enjoyed by U.S. personnel having diplomatic status except for circumstances in which there is a substantial risk of terrorist acts.)

b. **Unofficial Travel.** All persons having access to SCI who plan unofficial travel to, through, or within countries listed in the attached Appendix must:

(1) give advance notice of such planned travel;

(2) obtain a defensive security briefing from the specified official prior to performing such travel;

(3) contact immediately the nearest U.S. Consul, Attache, or Embassy Regional Security Officer or Post Duty Officer if detained or subjected to significant harassment or provocation while traveling; and

(4) report to the specified official upon return from travel any unusual incidents, including incidents of potential security concern, encountered during such travel. (Department and Agency personnel should be encouraged to report incidents of security concern they encounter in other countries as well.)

Failure to comply with the above provisions may result in the withdrawal of approval for continued access to SCI:

c. **Specific and Extensive Knowledge.** Persons with specific and extensive knowledge of the following aspects of foreign intelligence shall be advised that unofficial travel without the approval of the cognizant SOIC may result in the withdrawal of approval for continued access to SCI:

(1) technological structure, function, and techniques of sensitive intelligence collection or exploitation system/methods;

(2) designated system targets or sources;

(3) method and purpose of target selection;

(4) degree of success of collection or exploitation system/method; or

(5) collection of exploitation system/method capabilities and vulnerabilities.

d. **Previous Access.** Persons whose access to SCI is being terminated will be officially reminded of their continuing obligation to protect SCI and will be afforded advisories on the risks associated with participation in hazardous activities.

4. Responsibilities

a. The DCI will cause to be prepared and disseminated to the SOICs a list of countries identified as posing a security risk bearing on this policy (see Appendix). The Security Committee shall coordinate required support including source material concerning these risks.

b. SOICs shall issue implementing directives concerning travel and assignment of personnel of their departments or agencies. Such directives shall include the overall policy, definitions, and criteria set forth herein and provide for:

(1) an annual reminder of the policy set forth in paragraph 3, above;

(2) defensive security briefings or risk of capture briefings to personnel of their departments or agencies;

(3) institution of positive programs for the collection of information reported under the provisions of paragraph 3b(4), above

(4) ensuring that new information obtained by their departments or agencies on incidents of security concern (e.g. harassments,

provocations or terrorist actions), or on risk of capture situations, is provided to the DCI Security Committee and to other interested NFIB agencies.

(5) Ensuring that recommendations for changes to the Appendix hereto are made to the DCI Security Committee and provide justification for addition or deletion of countries.

5. Classification

As this directive sets forth security policy for persons with access to SCI, it is classified CONFIDENTIAL in its entirety. Selected paragraphs may be excerpted for use at the FOR OFFICIAL USE ONLY level by SOICs, their designees, or SCI Special Security/Control officers, when considered appropriate. The identification of any country in the Appendix as having been designated as a hazardous area by the DCI is classified CONFIDENTIAL.

(DRAFT)

William J. Casey

Attachment:

Countries and Areas in Which Visits, Travel, and Assignment are Considered to be a Hazardous Activity.

Date

ROUTING AND TRANSMITTAL SLIP

TO: (Name, office symbol, room number, building, Agency/Post)	Initials	Date
1. DD/S FYI		10 DEC 1984
2. D/S		12 DEC 1984
3.		
4.		
5.		

Action	File	Note and Return
Approval	For Clearance	Per Conversation
As Requested	For Correction	Prepare Reply
Circulate	For Your Information	See Me
Comment	Investigate	Signature
Coordination	Justify	

REMARKS

DO NOT use this form as a RECORD of approvals, concurrences, disposals, clearances, and similar actions

STAT

[redacted] gency/Post) DD/PTAS	Room No.—Bldg.
	Phone No.

5041-102

OPTIONAL FORM 41 (Rev. 7-76)
Prescribed by GSA
FPMR (41 CFR) 101-11.206

☆ GPO: 1983 O - 381-529 (232)

ROUTING AND TRANSMITTAL SLIP Date 12/6/84

TO: (Name, office symbol, room number, building, Agency/Post)	Initials	Date
1. C/SSC/OS		
2. NO PROBLEM - NO ACTION - NO SUBSTANTIAL PROGRESS !		
3.		
4.		

5.

Action	File	Note and Return
Approval	For Clearance	Per Conversation
As Requested	For Correction	Prepare Reply
Circulate	For Your Information	See Me
Comment	Investigate	Signature
Coordination	Justify	

REMARKS

25X1

Personally, I see no problem with the attached. The policies are already "in place" in EAB, SSC, SAG, OSB and industry. Shall we give it a "go"? (PPG will do the response.)

DO NOT use this form as a RECORD of approvals, concurrences, disposals, clearances, and similar actions

25X1

From: (Name, org. symbol, Agency/Post)	Room No.—Bldg.
	Phone No.

OPTIONAL FORM 41 (Rev. 7-76)
Prescribed by GSA
FPMR (41 CFR) 101-11.206

☆ GPO: 1983 O - 381-529 (232)