

ORDER

U.S. DEPARTMENT OF TRANSPORTATION
FEDERAL AVIATION ADMINISTRATION

1600.61A

11/03/00

**SUBJ: FOREIGN TRAVEL BRIEFING & CONTACT REPORTING REQUIREMENTS FOR FAA
AND CONTRACTOR EMPLOYEES**

1. PURPOSE. This order establishes security briefing requirements for FAA and contractor employees prior to travel to foreign countries on official and unofficial business, and requirements for reporting certain contacts with foreign nationals. It implements provisions of Order DOT 1640.4D, Classified Information Management, and Presidential Decision Directive (PDD) 12, Security Awareness and Reporting of Foreign Contacts.

2. DISTRIBUTION. This order is distributed to all managers in FAA headquarters, regions, centers, field offices, and facilities.

3. CANCELLATION. Order 1600.61, Defensive Security Briefing Requirements for FAA Employees Traveling to Communist-Controlled Countries, dated November 30, 1982, is canceled.

4. EXPLANATION OF CHANGES. This order:

a. Implements DOT requirements for foreign travel briefings and reporting certain contacts with foreign nationals.

b. Establishes specific time frames for providing the required briefings.

c. Broadens the scope of this order to encompass persons under contract or agreement with the FAA.

d. Changes the title of the order to reflect current dual requirements.

e. Eliminates specific briefing requirements for travel to particular countries and the use of DOT Form 1630-6, Defensive Security Briefing Certificate, which is now obsolete.

5. BACKGROUND.

a. In carrying out the FAA's mission, FAA and contractor employees sometimes travel on agency business to countries whose interests are not entirely in concert with those of the United States (U.S.) or to countries where there are criminal or terrorist threats to their safety. Innocent travel and tourist activities, often perfectly acceptable in the U.S., may be seized upon by other nations as a basis for the arbitrary arrest or detention of travelers, and as a means of embarrassing the travelers and the U.S. All

U.S. Government and contractor employees, regardless of agency, position, or assignment, are of particular interest because of their association with the U.S. and/or awareness or actual knowledge of information that could be used to enhance the military, technological, or economic strength of a foreign country. Even a limited amount of information, whether classified or not, could be combined with information from other sources to the advantage of a foreign country or detriment of the U.S.

b. PDD 12 states that foreign intelligence services (FIS) continue to acquire classified or otherwise sensitive information and recruit personnel believed to have access to such information despite the end of the Cold War and the collapse of the former Soviet Union. These intelligence services are associated with and operate in countries considered friendly to the U.S. as well as countries whose interest is generally considered inimical to those of the U.S. Most FIS cultivate friendships to create an assessment period before actual recruitment or exploitation of a person. The majority of such contacts can appear to be innocent social encounters or requests for "unimportant" information.

c. Terrorist groups, foreign nationals, and private industry can present a threat to FAA and contractor employees through random violence and attempts to obtain FAA sensitive, proprietary, and classified information. Only those who are aware of this threat will recognize when they are being targeted for any purpose and when they are being manipulated toward involvement in intelligence or terrorist activities.

6. AUTHORITY TO CHANGE THIS ORDER. The Associate Administrator for Civil Aviation Security is authorized to issue changes to this order which do not establish or revise policy, delegate authority, or assign responsibility.

7. DEFINITIONS.

a. Defensive Security Briefing. A formal briefing that alerts the recipient to the potential for harassment, exploitation, provocation, capture, or entrapment. The briefing includes information on courses of action helpful in mitigating adverse security and personnel consequences and advice on passive and active measures that personnel should take to avoid becoming targets or inadvertent victims while on foreign travel. (Refer to Director of Central Intelligence Directive 1/20, Security Policy Concerning Travel and Assignment of Personnel with Access to Sensitive Compartmented Information (SCI)).

b. Foreign National. A person who is not a citizen or national of the U.S..

c. Official Travel. Travel performed at the direction of the U.S. Government.

d. Senior Officials of the Intelligence Community (SOIC). The heads of organizations within the Intelligence Community or their designated representatives.

e. Sensitive Compartmented Information (SCI). All intelligence information and material that requires special controls for restricted handling within compartmented channels and for which compartmentation is established.

f. Servicing Security Element (SSE). The organization responsible for providing security services to Washington headquarters, regions, and centers. These elements are the Office of Civil Aviation Security Operations (ACO) in the Washington headquarters, the Civil Aviation Security Divisions in the regions, and at the Aeronautical Center and the Civil Aviation Security Staff at the Technical Center.

g. Unofficial Travel. Travel undertaken by an individual without official, fiscal, or other obligations on the part of the U.S. Government.

8. POLICY.

a. A security briefing is required for each FAA employee prior to his/her departure for any foreign country on official business, unless he/she has received a briefing within 12 months of the date of departure.

b. All FAA and contractor employees shall be made aware, through a security briefing, of situations they could encounter while on travel to foreign countries and of basic defensive measures they can take against these threats. Each person shall conduct himself/herself in such a manner that prevents personal and professional compromise and shall do everything possible to avoid involvement in situations that might embarrass the U.S. and/or the FAA.

9. RESPONSIBILITIES.

a. Associate Administrator for Civil Aviation Security, ACS-1, is responsible for the overall implementation of the provisions of this order and, as necessary, providing updated information for security briefings.

b. Office of Civil Aviation Security Policy and Planning, ACP-1, is responsible for developing policy and guidance to implement DOT requirements for foreign travel briefings and for reporting contacts with foreign nationals and all suspicious contacts.

c. Office of Civil Aviation Security Operations, ACO-1, is responsible for ensuring that SSE's assist supervisors and employees in complying with the provisions of this order and for providing oversight of this program throughout FAA.

d. Director, Office of Civil Aviation Security Intelligence/SOIC, ACI-1, or his/her designee is responsible for notifying each FAA employee with access to SCI when special security briefings are required for travel to a foreign country and for providing these briefings.

e. Service Security Elements are responsible for assisting supervisors, operating offices, and FAA employees in complying with this order.

f. Operating Offices shall ensure all contractor employees, and other persons by agreement with the FAA, who work in or have access to FAA facilities, sensitive information, and/or resources for which they are responsible:

(1) Are made aware of the provisions of this order at least 14 days prior to traveling to a foreign country.

(2) In the case of short-notice (less than 14 days prior to expected departure date) foreign travel, are made aware of the provisions of this order as soon as practicable prior to departure.

(3) Certify in writing that they have been made aware of the provisions of this order by signing and dating the certification found in Appendix 1, Guide for Employees Traveling to Foreign Countries.

(4) Receive a copy of appendix 1 upon request.

g. Supervisors shall ensure that FAA employees:

(1) Are made aware of the provisions of this order at least 14 days prior to traveling to a foreign country.

(2) In the case of short-notice (less than 14 days prior to expected departure date) foreign travel, are made aware of the provisions of this order as soon as practicable prior to departure.

(3) Certify, in writing, that they have been made aware of the provisions of this order by signing and dating the certification form found in appendix 1.

(4) Receive a copy of appendix 1 upon request prior to personal, unofficial travel to a foreign country.

h. Employees shall report to their managers and their SSE any contact with individuals of any nationality who seek illegal or unauthorized access to classified or sensitive information, either while in a foreign country or in the U.S. Employees shall also report to the SSE any concerns they have that they may be the targets of actual or attempted exploitation by a foreign entity.

10. TARGET RECOGNITION.

a. FAA and contractor employees should be aware that an intelligence agency, security service, terrorists, criminals, or a competitor could target them if they are believed to be U.S. citizens and/or knowledgeable of, or carrying information concerning, but not limited to, the following:

(1) Facilities and systems for air navigation and control of air traffic, particularly the capabilities and vulnerabilities of these systems.

(2) How the FAA protects its critical infrastructure, especially from deliberate attempts to disrupt the national airspace system and/or FAA operations.

(3) Technologies that may not be readily available in other countries or on which there are export restrictions.

(4) The FAA's interactions with foreign governments, including proposed agreements, contracts, and other working relationships.

- (5) Information a foreign government shares with the FAA in confidence.
- (6) FAA support provided to classified or sensitive military operations or law enforcement activities.
- (7) Sensitive security information (SSI) as defined in 14 CFR Part 191, Sensitive Security Information.
- (8) Intelligence activities, intelligence methods or sources, and communications security (COMSEC) equipment, keying material, and operating procedures.
- (9) Classified information or other matters related to the national security.

b. These are indicators of unwarranted interest that each FAA and contractor employee should be familiar with:

- (1) Repeated contacts with a foreign national or other individual who is not involved in your business interests or the purpose of your visit, but as a result of invitations to social or business functions appears at each function. This individual's demeanor may indicate more than just a passing interest in you or your business activities.
- (2) Establishment of close social relationships with representatives of a foreign government for business reasons that begin to develop beyond the business level.
- (3) Accidental encounters with unknown foreign nationals or other unknown persons who strike up a conversation and want to talk about the U.S., politics, your employment, etc. The individual may try to use other excuses to begin a "friendly" relationship.
- (4) Any unauthorized solicitation of classified, sensitive, or proprietary information.
- (5) Unusual interest in specific duties, functions, or responsibilities of an individual, position, office, unit, or agency.
- (6) Unusual or repeated requests for seemingly "unimportant" information.
- (7) Any events that suggest targeting of FAA personnel, facilities, or resources by a FIS or terrorist group.
- (8) Any offer to provide you classified or sensitive information.
- (9) All information regarding the intentions of terrorist organizations.
- (10) All information regarding planned or actual acts of sabotage or subversion.

11. GENERAL SECURITY BRIEFING REQUIREMENTS.

- a. Each FAA and contractor employee must receive a security briefing within 14 days prior to departure for any travel to a foreign country on official business.
- b. Each FAA and contractor employee must receive a security briefing concerning the reporting of certain contacts and incident information annually.
- c. The briefing need not consist of anything other than a reading of Appendix 1, Guide for Employees Traveling to Foreign Countries, which contains the information required for this briefing.
- d. Regional Security Officer will provide security awareness information to those FAA and contractor employees who are permanently assigned to a U.S. diplomatic mission.
- e. Employees are encouraged to check Travel Warnings and Public Announcements and Consular Information sheets issued by the Bureau of Consular Affairs, Department of State, for countries that they plan to visit. This information is available on the State Department's web site, <http://travel.state.gov>, or can be obtained by calling Overseas Citizens Services, 202-647-5225.

12. SPECIAL SECURITY BRIEFING REQUIREMENTS. The Central Intelligence Agency (CIA) grants certain FAA employees access to SCI. Persons granted access to SCI incur a special security obligation and, with the exception of official travel, are discouraged from traveling to countries that pose a threat to SCI and/or SCI indoctrinated personnel. In accordance with Director of Central Intelligence Directive (DCID) 1/20, all SCI holders must notify ACI-1 in writing of all foreign travel. SCI indoctrinated travelers must be alerted to the risks associated with foreign travel. Failure to comply with the following provisions may result in the withdrawal of approval for continued access to SCI and may be considered in determining whether to grant future SCI access approvals.

- a. Official Travel. Employees with access to SCI engaging in official travel shall:
 - (1) Submit an itinerary in writing to ACI-1 within 14 days prior to the date of travel.
 - (2) Attend a Defensive Security and/or a Risk of Capture briefing as determined by ACI-1 within 14 days prior to travel, as necessary.
 - (3) Report to ACI-1 any unusual incidents or contacts as described in paragraph 10.
- b. Unofficial Travel. Employees with access to SCI engaging in unofficial travel shall:
 - (1) Submit an itinerary in writing to ACI-1 within 14 days prior to the date of travel unless the travel is due to a personal emergency.
 - (2) Attend a Defensive Security and/or a Risk of Capture briefing if determined by ACI-1 as necessary.

(3) Be advised that such travel without cognizant SOIC approval may result in the withdrawal of approval for continued access to SCI.

(4) Report to ACI-1 any unusual incidents or contacts as described in paragraph 10.

13. CONTACT AND INCIDENT REPORTING REQUIREMENTS.

a. FAA and contractor employees shall report to their SSE any contact with a foreign national that would appear to be an attempt to obtain unauthorized access to classified, sensitive, or proprietary information or technology and/or the possibility of continued contact with such an individual.

b. SSE's shall review and evaluate all information reported by FAA and contractor employees and report to the Office of Security and Administrative Management (M-40), Office of the Secretary, through the Investigations Division (ACO-300), any facts or circumstances of a reported contact or incident that would appear to meet one of the criteria in paragraph 10a (1) and (2), or 10b.

14. CLASSIFIED INFORMATION. FAA and Contractor employees who need access to classified information during travel outside of the U.S., who need to transfer it outside of the U.S., or who need to send it back to the U.S. from a foreign country, shall follow the requirements and procedures contained in the latest edition of Order 1600.2, Safeguarding Controls and Procedures for Classified National Security Information and Sensitive Unclassified Information.

15 - 199. RESERVED.



William S. Davis

Acting Associate Administrator for Civil Aviation Security