Department of Homeland Security
Management Directives System
MD Number: 11039
Issue Date: 07/14/2006

FOREIGN TRAVEL REPORTING REQUIREMENTS FOR INDIVIDUALS GRANTED ACCESS TO SENSITIVE COMPARTMENTED INFORMATION

I. Purpose

This Management Directive (MD) establishes the reporting requirements for individuals granted access to Sensitive Compartmented Information (SCI) who will undertake either official or unofficial foreign travel.

II. Scope

This MD applies to all of DHS.

III. Authorities

This MD is governed by numerous Public Laws, regulations, rules, and other MDs, including but not limited to:

A. Public Law 107-296, “Homeland Security Act of 2002.”

B. Executive Order 10450, as amended, “Security Requirements for Government Employment,” April 27, 1953.

C. Executive Order 12829, as amended, “National Industrial Security Program,” January 6, 1993.

D. Executive Order 12958, as amended, “Classified National Security Information,” April 17, 1995.

E. Executive Order 12968, as amended, “Access to Classified Information,” August 2, 1995.

F. Presidential Decision Directive – 12, “Security Awareness and Reporting of Foreign Contacts,” August 5, 1993.

G. Director of Central Intelligence Directive (DCID) 1/20, “Security Policy Concerning Travel and Assignment of Personnel with Access to Sensitive Compartmented Information (SCI),” December 29, 1991.

H. Director of Central Intelligence Directive 6/1, “Security Policy for Sensitive Compartmented Information and Security Policy Manual,” March 1, 1995.

I. Director of Central Intelligence Directive 6/4, “Personnel Security Standards and Procedures Governing Eligibility for Access to Sensitive Compartmented Information (SCI),” July 2, 1998.

J. Director of Central Intelligence Directive 6/9, “Physical Security Standards for Sensitive Compartmented Information Facilities,” November 18, 2002.

K. Designation of Chief Security Officer as Senior Agency Official, March 3, 2004.

L. Delegation of Authorities from the Assistant Deputy Director of National Intelligence for Security to Chief Security Officer, Department of Homeland Security, March 13, 2006.

M. DHS Delegation Number 8150, “Delegation to Chief, Office of Security of Determination Authority and Cognizant Security Authority.”

N. DHS Management Directive 11043, “Sensitive Compartmented Information Program Management,” dated September 17, 2004.

IV. Definitions

A. ***Cognizant Security Authority (CSA)***: As defined in Director of Central Intelligence Directive (DCID) 6/9, “Physical Security Standards for Sensitive Compartmented Information Facilities,” the CSA is the individual designated by a Senior Official of the Intelligence Community (SOIC) to serve as the responsible official for security program management with respect to protection of intelligence sources and methods under SOIC responsibility.

B. ***Components***: All the entities that directly report to the Office of the Secretary, which includes the Secretary, Counselors and their staff, Deputy Secretary and his or her staff, and Chief of Staff and his or her staff.

C. ***Contact***: Any form of meeting, association, or communication in person, by radio, telephone, letter, computer, or other means, regardless of who initiated the contact, for social, official, private, or other reasons.

D. ***Country-Specific Briefing***: A formal briefing that alerts the recipient to country specific security, safety, or intelligence threats.

E. ***Defensive Security Briefing***: A formal briefing that alerts the recipient to the potential for harassment, exploitation, provocation, capture, entrapment, bodily injury or death.

F. ***Foreign National***: A person who is not a citizen or national of the United States.

G. ***Foreign Travel***: Travel outside the United States, its Territories, or Possessions.

H. ***Incident of Security Concern***: Indicators that an organization or foreign government may be targeting an individual in an attempt to gain access to classified national security or sensitive U.S. Government information. Incidents can be subtle or direct and may be overtly or covertly undertaken. Incidents of Security Concern which must be reported by SCI-indoctrinated personnel include, but are not limited to:

1. Attempts by unauthorized persons (foreign national or U.S. citizen) to gain access to classified national security information or sensitive but unclassified information;

2. Planned, attempted, actual, or suspected terrorism, espionage, sabotage, subversion or blackmail attempt; contact with a known or suspected foreign intelligence service; and

3. Unusual or repeated requests for seemingly "unimportant" information; repeated contact with a foreign national or other individual who is not involved in your business interests or in the purpose of your visit, but as a result of invitations to social or business functions, appears at each function; and any event which the SCI-indoctrinated individual wishes to make a matter of record. [See definition of Contact above.]

I. ***Intelligence Community (IC)***: As defined by National Security Act of 1947, as amended, the IC is a federation of executive branch agencies and organizations that conduct intelligence activities necessary for the conduct of foreign relations and the protection of the national security of the United States.

J. ***Official Travel***: Travel performed at the direction of the U.S. Government, required by a Government contract or specifically approved by a DHS Program Manager.

K. ***Senior Agency Official***: The individual designated by the agency head under section 5.4(d) of E.O. 12958, as amended, who directs and administers the agency's program under which information is classified, safeguarded, and declassified. The Senior Agency Official for DHS is the Chief Security Officer.

L. ***Sensitive Compartmented Information (SCI)***: SCI is classified information concerning or derived from intelligence sources, methods or analytical processes, which is required to be handled exclusively within formal control systems as directed by the Director of National Intelligence.

M. ***Special Security Officer (SSO)***: An individual who works under the direction of the Chief, Special Security Programs Division and administers the receipt, control and accountability of SCI. The SSO oversees SCI security functions and reporting requirements within their assigned Component.

N. ***Special Security Representative (SSR)***: An individual who works under the direction of the supporting SSO, and is responsible for the day-to-day management and implementation of SCI security and administrative instructions for an assigned area of responsibility.

O. ***Unofficial Travel***: Travel other than official travel, undertaken at the personal discretion of an individual.

V. Responsibilities

A. ***The Chief Security Officer (CSO)*** is the Cognizant Security Authority and Senior Agency Official for the Department. As such he/she is responsible for:

1. The overall implementation of the provisions of this MD and, as necessary, providing updated information for security briefings; and

2. Establishing programs for the collection and analysis of information reported pursuant to this MD and sharing that information and analysis with the IC.

B. ***The U.S. Coast Guard*** shall independently administer its foreign travel reporting requirements for individuals granted access to SCI.

C. ***Chief, Special Security Programs Division, DHS Office of Security*** is responsible for:

1. Managing the security-related requirements for SCI programs within DHS except for the U.S. Coast Guard.

2. Maintaining copies of DHS Form 11043-1 in accordance with the Federal Records Act.

D. ***Chief, Internal Security and Investigations Division, DHS Office of Security*** is responsible for:

1. Identifying, analyzing, and counteracting espionage, foreign intelligence elicitation activities, and terrorist collection efforts directed against DHS SCI indoctrinated employees, detailees, and contractors on official or unofficial foreign travel; and

2. Assessing and analyzing an Incident of Security Concern reported pursuant to this MD.

E. ***Component SSOs and SSRs*** are responsible for:

1. Ensuring that SCI-indoctrinated employees, detailees, or contractors within their Component or area of responsibility report foreign travel on DHS Form 11043-1 “Notification of Foreign Travel”;

2. If necessary, providing Defensive Security Briefing or Country-Specific Briefing to SCI-indoctrinated employees, detailees, and contractors traveling abroad to include coordinating with the Chief, Internal Security and Investigations Division to obtain briefing materials regarding specific threats or concerns impacting DHS personnel;

3. Forwarding copies of DHS Form 11043-1 to the Office of Security, Special Security Programs Division;

4. Forwarding a copy of each completed DHS Form 11043-1 to the personnel security office that adjudicated the individual’s SCI clearance; and

5. Coordinating with the Chief, Internal Security and Investigations Division any Incidents of Security Concern reported by SCI-indoctrinated employees, detailees, or contractors.

VI. Policy & Procedures

A. ***Policy***: Individuals granted access to SCI by DHS incur a special security obligation and will comply with all applicable foreign travel reporting requirements, including those issued by the Director of National Intelligence. Non-compliance by federal employees with the reporting requirements in this MD may result in revocation of access to SCI, discipline, and/or discharge.

B. ***Procedures***: Individuals granted access to SCI by DHS must:

1. Complete and submit DHS Form 11043-1 to their SSO or SSR thirty (30) days prior to foreign travel. In the event of unanticipated or emergency travel submit DHS Form 11043-1 as soon as practical; and

2. Immediately upon their return from foreign travel, report all Incidents of Security Concern to their servicing SSO or SSR. If the incident requires a response while on travel, contact the Regional Security Officer at the nearest U.S. Embassy or Consulate.

3. Individuals granted access to SCI by the U.S. Coast Guard will report foreign travel in accordance with established U.S. Coast Guard procedures.

VII. Questions

Address questions regarding this MD to the DHS Office of Security.