Transportation Security Administration

OFFICE OF LAW ENFORCEMENT/ FEDERAL AIR MARSHAL SERVICE

TSA MANAGEMENT DIRECTIVE No. 2800.5
INTERNAL SECURITY REPORTING: FOREIGN CONTACT AND TRAVEL

To enhance mission performance, TSA is committed to promoting a culture founded on its values of Integrity, Innovation and Team Spirit.

REVISION: This revised directive supersedes TSA MD 2800.5, *Internal Security Reporting: Foreign Contact and Travel, dated November 2, 2009.*

SUMMARY OF CHANGES: Section 3, Authorities, changes reference from Executive Order (EO) 12958 to EO 13526.

1. **PURPOSE:** This directive provides TSA policy and procedures for TSA employees and contractors regarding official and unofficial travel to foreign countries and for reporting unusual or suspicious contacts with foreign nationals in relation to internal security issues and foreign intelligence elicitation attempts.

2. **SCOPE:** This directive applies to all TSA employees and contractors who work in the U.S. and its territories as well as those posted overseas. Further, TSA employees or contractors, whether permanently assigned or on temporary duty (TDY) for 25 days or more to an overseas location which is under the authority of a Chief of Mission, are subject to additional requirements for advance notification of foreign travel and timely reporting of foreign contacts under Department of State regulations.

3. **AUTHORITIES:**

   A. 49 CFR Part 1520, *Protection of Sensitive Security Information*

   B. EO 10450, as amended, *Security Requirements for Government Employment*

   C. EO 12968, as amended, *Access to Classified Information*

   D. EO 13526, *Classified National Security Information*

   E. DHS MD 11039, *Foreign Travel Reporting Requirements for Individuals Granted Access to Sensitive Compartmented Information*

   F. DHS MD 11052, *Internal Security Program*

   G. DHS MD 11060.1, *Operations Security Program*

   H. Department of State, 12 Foreign Affairs Manual (FAM) 260, *Counterintelligence*

   I. Department of State, 6 Foreign Affairs Handbook (FAH)-5 H-351, *Direct-Hire Personnel*

J. Presidential Decision Directive/National Security Council (PDD/NSC)-12, *Security Awareness and Reporting of Foreign Contacts*

K. Director of Central Intelligence Directive (DCID) 1/19, *Security Policy for Sensitive Compartmented Information and Security Policy Manual*

L. DCID 1/20, *Security Policy Concerning Travel and Assignment of Personnel with Access to Sensitive Compartmented Information (SCI)*

M. Intelligence Community Directive (ICD) 704, *Personnel Security Standards and Procedures Governing Eligibility for Access to Sensitive Compartmented Information and Other Controlled Access Program Information*

N. Title I of Pub. L. 99-399, *The Omnibus Diplomatic Security and Antiterrorism Act* of 1986, as amended, codified at 22 U.S.C., Section 4801 et seq.

4. DEFINITIONS:

A. Chief of Mission: The principal officer in charge of a diplomatic mission of the United States or of a United States office abroad which is designated by the Secretary of State as diplomatic in nature, including any individual assigned to be temporarily in charge of such a mission or office. Chiefs of Mission titles may include the following: Ambassador, Chargé d'Affaires, or Consul General.

B. Defensive Activities: Activities relating to personnel, physical, document, and communications security, such as training and awareness, foreign travel/contact briefings and debriefings, foreign visitor management, threat analysis, coordination with appropriate Intelligence Community members and law enforcement agencies, internal security incident/indicator reporting, security issue reviews as coordinated with proper authorities, and assistance to adjudications and security disciplines.

C. Department of State Contractor: A U.S. personal services contractor serving under the authority of a Chief of Mission or an employee of a commercial firm having a contract with the U.S. Government and serving under the authority of a Chief of Mission.

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

E. Foreign Service National (FSN): A non-U.S. citizen from the host country or a third-country national who is hired to work at an American Embassy or Consulate located in a foreign country.

F. Official Travel: Travel performed at the direction of the U.S. Government.

G. Regional Security Officer (RSO): Diplomatic Security Service (DSS) Special Agent serving overseas as the head of security at an American Embassy. Working for the U.S. Department of State as Special Agents, RSOs are also considered officers within the State Department acting as specialists within the Foreign Service of the United States. The RSO administers security services (e.g., delivering briefings and reviewing foreign contact reports) and advises the

Ambassador on all security matters to protect Foreign Service personnel, facilities, operations and information against hostile intelligence, criminal, and terrorist activities.

H. 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.

I. Unofficial Travel: Travel undertaken by an individual without official, fiscal, or other obligations of the U.S. Government which can also be referred to as personal or leisure travel.

5. RESPONSIBILITIES:

A. The Chief Security Officer (CSO), Office of Security, Office of Security Services and Assessments (OSSA), Office of Law Enforcement/Federal Air Marshal Service (OLE/FAMS) is responsible for oversight and direction of the provisions of this directive. The CSO may delegate the authority to establish and implement the TSA foreign travel and foreign contact reporting and briefing/debriefing procedures in accordance with DHS Internal Security and Special Security Programs.

B. The TSA Internal Security Program Manager, Office of Security, OSSA, OLE/FAMS is responsible for:

(1) Ensuring that this directive is disseminated to all employees and contractors annually as required training through the TSA Online Learning Center (OLC).

(2) Compiling and evaluating all reports of foreign contacts in his/her capacity as the point of contact for internal security matters including the development of internal security activities and awareness training for TSA.

(3) Advising the TSA CSO and DHS Internal Security Program Manager when information indicates that classified information is being, or may have been, disclosed in an unauthorized manner to a foreign national or an agent of a foreign government, as well as other unusual foreign contact incidents.

(4) Forwarding foreign contact reports received from Operations Security (OPSEC) facilitators to the TSA Office of Inspection and, when warranted, to the DHS Counterintelligence (CI) and Investigations Division.

(5) Coordinating and assisting other TSA offices and Federal agencies on defensive activities, inquiries and investigations.

C. The Special Security Officer (SSO), Office of Security, OSSA, OLE/FAMS is responsible for providing TSA employees and contractors who have access to SCI with special security briefings prior to ***any*** travel to a foreign country.

D. OPSEC facilitators or other designated employees are responsible for monitoring and archiving reports of unusual or suspicious contacts with foreign nationals submitted by TSA personnel in their assigned area of responsibility. These reports shall be forwarded, as soon as practicable, to

the TSA Internal Security Program Manager (OPSEC.TSA@dhs.gov) for recordkeeping and analyses.

NOTE: OPSEC facilitators must hold a minimum of a SECRET security clearance because details of a foreign contact report may potentially result in the disclosure of classified information or actions.

E. TSA employees, contractors, supervisors, rating officers or other employees with firsthand knowledge of security concerns involving another TSA employee or contractor are responsible for bringing the matter to the attention of appropriate agency officials. Examples of a security concern may include the following: knowledge of a close social relationship with a representative of a foreign government that begins to develop beyond a professional association; repeated encounters with a foreign national at social or business functions who aggressively seeks out contact not in keeping with the level of the event or situation; and, an ongoing personal relationship with a foreign national who has not been previously subjected to a U.S. Government background check for criminal or terrorist affiliations.

6. POLICY:

A. An Internal Security Training and Awareness Program is required training for all DHS employees on topics such as foreign intelligence service elicitation and recruitment techniques, potential espionage indicators, terrorist modus operandi, espionage case studies, and internal security reporting requirements and processes.

(1) All TSA employees and contractors must complete initial training within 30 days of enter-on-duty (EOD) to TSA and annual refresher training, whether or not the individual is required to conduct foreign travel for his/her position. Reading and acknowledging the responsibilities specified in this directive through the TSA OLC shall fulfill this requirement.

(2) If the OLC training cannot be accomplished for any reason before official travel takes place within the first 30 days of EOD, a supervisor or higher level manager may direct an individual to read this directive and sign and date it for internal record, as long as the individual is cognizant that the OLC training must be taken at the earliest opportunity upon return from travel.

B. TSA employees and contractors granted access to SCI incur special security obligations and, with the exception of official travel, are discouraged from traveling to countries that pose an intelligence collection threat to SCI and/or SCI indoctrinated personnel. In accordance with DHS MD 11039, *Foreign Travel Reporting Requirements for Individuals Granted Access to Sensitive Compartmented Information,* TSA employees and contractors granted access to SCI, whether based in the U.S. or at a foreign location under a Chief of Mission, traveling for either official or unofficial reasons to any foreign country, must notify the TSA SSO of all foreign travel. Failure to comply with this provision may result in the temporary or permanent termination of continued access to SCI and may be referred to the Personnel Security Division, Office of Security, when adjudicating future security clearance access.

C. **Non-SCI-indoctrinated TSA personnel based in the U.S. or its territories, to include Federal Air Marshals (FAMs), are not required to notify their first-line supervisor or**

other TSA office of any official or unofficial foreign travel for purposes of this directive. This statement, however, does not override any other TSA requirements to report official travel through separate channels.

D. TSA employees or contractors, whether permanently assigned or on temporary duty (TDY) for 25 days or more to an overseas location which is under the authority of a Chief of Mission, are subject to additional requirements for advance notification of foreign travel and timely reporting of foreign contacts under the following Department of State regulations: 12 Foreign Affairs Manual (FAM) 262, *Security Awareness and Contact Reporting*, as found in 12 FAM 260; and 12 FAM 264, *Personal Travel to Critical Human Intelligence Threat Countries*, as found in 12 FAM 260. This includes notifying the Regional Security Officer (RSO) at post of residence in advance of intended personal travel to any destination widely recognized as posing a security threat to the United States and its citizens (i.e., any country with a "critical human intelligence threat post"), including travel with tour groups. If the traveling employee is unsure as to whether the country of destination falls under this category, he/she must contact the State Department or RSO for more information regarding countries that are considered a critical threat. Failure to comply with the requirements of this directive may result in administrative or other punitive actions against the employee or contractor.

E. A reporting and briefing/debriefing procedure is required for all unusual or suspicious foreign contacts. Reports of these types of foreign contacts are required whether the incident or association occurs within the U.S. and its territories or at a foreign location.

(1) In PDD/NSC-12, the President of the United States has directed that each department or agency of the U.S. Government establish procedures, in consultation with the Department of Justice, requiring its employees to report all contacts with individuals of any nationality, either within or outside the scope of the employee's official activities, whenever:

(a) Illegal or unauthorized access is sought to classified or otherwise sensitive information; *or*

(b) The employee is concerned that he or she may be the target of actual or attempted exploitation by a foreign entity.

(2) TSA employees and contractors with SCI clearance, whether based in the U.S. or at a foreign location under a Chief of Mission, shall report all foreign contacts to the TSA SSO in accordance with DHS MD 11039.

(3) Employees must also report any initial contact with a national from a country that the U.S. Government considers to be a critical human intelligence threat whenever that individual attempts to establish recurring contact or seems to be actively seeking a close personal association beyond professional or personal courtesies. For more information regarding countries that are considered a critical threat, contact the RSO for employees posted overseas or the TSA Office of Security for employees posted at domestic locations.

(4) As described in EO 10450, it is prohibited for U.S. Government employees to establish or continue "a sympathetic association with a saboteur, spy, traitor, seditionist, anarchist, or revolutionist, or with any espionage or other secret agent or representative of a foreign nation, or any representative of a foreign nation whose interests may be inimical to the

interests of the United States, or with any person who advocates 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." Failure to report these types of contact can result in immediate termination of employment as well as potential civil and/or criminal actions taken against the individual.

7. PROCEDURES:

A. Procedures for reporting travel to foreign destinations.

(1) All U.S. Government employees under the authority of a Chief of Mission must provide the RSO at post of residence with the itinerary at least three (3) weeks before starting travel, or as soon as practicable under extenuating circumstances dictated by operational necessity. Each employee must provide notification of personal travel by following the requirements of Department of State, 12 FAM 260, *Counterintelligence*.

(a) The RSO also ensures that each traveler receives a defensive security briefing prior to his/her travel.

(b) TSA employees or contactors under the authority of a Chief of Mission must immediately contact the nearest U.S. Consulate, Attaché, RSO or duty officer if detained or subjected to significant harassment or provocation while traveling.

(2) TSA SCI-indoctrinated personnel, whether based in the U.S. or at a foreign location under a Chief of Mission, must attempt to notify the TSA SSO at least one (1) week prior to departure. Should operational necessity or an unavoidable personal emergency requiring travel arise less than one (1) week prior to departure, notification can be made at any time before or after the travel by either the individual who is traveling or another TSA employee or assistant on behalf of the SCI-indoctrinated individual in order to ensure that the travel is recorded. Per DHS MD 11039, DHS Form 11043-1, *Notification of Foreign Travel*, is available to report the travel. DHS also promulgates a second authorized form, DHS Form 11053-1, *Notification of Foreign Travel*, for this purpose. Both forms can be located on the TSA Foreign Contact and Travel webpage. Completed forms must be sent to TSA-SSO@dhs.gov.

B. Procedures for reporting unusual or suspicious contacts with foreign nationals.

(1) An unusual or suspicious encounter can be described as any contact with a foreign national that would appear to be an attempt by the foreign national to obtain unauthorized access to classified, sensitive, and/or proprietary information or technology. Other types of situations that are subject to reporting are an ongoing personal relationship with a foreign national who has not been previously subjected to a U.S. Government background check for criminal or terrorist affiliations or if continuing contact with one or more foreign nationals through a personal association that may result in cohabitation or otherwise close, continuing and personal relationship.

(2) TSA employees and contractors, regardless of SCI clearance, whether based in the U.S. or at a foreign location under a Chief of Mission, must report an unusual or suspicious encounter as soon as practicable to their immediate supervisor, designated OPSEC

facilitator, and/or the TSA Internal Security Program Manager. SCI-indoctrinated TSA employees and contractors based in the U.S. or at a foreign location under a Chief of Mission are required to notify the TSA SSO in addition to the TSA points of contact. TSA Form 2823, *Foreign Contact Report*, is available for reporting these contacts. However, if the situation is time-sensitive, an e-mail message with the pertinent data may be sent until TSA Form 2823 can be completed at a later date. Additional reporting information can be found on the Foreign Contact and Travel webpage.

(a) TSA supervisors shall evaluate all reported information in order to determine if it meets any of the criteria in this directive and, if warranted, forward the information to the Internal Security Program Manager at TSA Headquarters at OPSEC.TSA@dhs.gov.

(b) If the information does not appear to meet the criteria, no further reporting to the Office of Security is necessary. It is recommended, however, that the report be retained in the supervisor's office for a minimum of one (1) year in the event that a counterintelligence investigation later becomes necessary.

(3) TSA employees and contractors who are permanently assigned or on TDY for 25 days or more to U.S. missions overseas shall follow instructions in section 12 FAM 262, *Security Awareness and Contact Reporting*, as found in 12 FAM 260, for reporting contacts experienced overseas.

(a) The RSO gives an arrival briefing on counterintelligence issues of concern to all employees and contractors assigned to post on permanent change of station. TDY personnel shall be briefed on contact reporting responsibilities and other counterintelligence issues, as appropriate, but in every case if the TDY is over 25 days. The RSO is also available to brief adult dependents of employees and contractors on a voluntary basis.

(b) TSA employees and contractors should report immediately any contacts with individuals of any nationality under circumstances referred to in Section 6.E. of this MD. In general, employee and contractor reporting should occur within one (1) business day after such contact has occurred. If unable to report within this time frame, or unsure about the need to report at all, employees and contractors at post should notify the RSO as soon as practicable. If the RSO is unavailable, employees and contractors should notify the administrative officer or the Deputy Chief of Mission.

(c) Employees to whom the FAM regulations apply shall use Form DS-1887, *Contact Reporting Form*, as found in 12 FAM 260, to report all contacts for which reports are required. If the official duty station is a U.S. Mission abroad, the report must be submitted to an RSO. When an employee reports a contact, the RSO will conduct checks to determine if information is available indicating that the foreign national has a background connected with intelligence gathering.

(d) It is not necessary to report contacts with local hire employees at post. These employees are referred to as Foreign Service Nationals (FSNs) and have undergone U.S. Government background checks for criminal and terrorist affiliations.

(e) For travel outside the post of residence, TSA employees and contractors should report any unusual incidents, including those of potential security concerns, to the RSO as soon as practicable upon return.

(f) RSOs will conduct departure security debriefings for all employees and contractors completing a tour of duty overseas.

C. A table summary of the requirements for notification of foreign travel and for reporting contact with foreign national(s) can be found on the Foreign Contact and Travel webpage.

8. EFFECTIVE DATE AND IMPLEMENTATION: This policy is approved and effective the date of the signature unless otherwise specified.

APPROVAL

Signed May 19, 2011

_____ _____
Robert S. Bray Date
Assistant Administrator for Law Enforcement/
Director of the Federal Air Marshal Service

EFFECTIVE

_____
Date

Distribution: All TSA Employees and Contractors, Assistant Administrators and equivalents, Managers and Supervisors, BMO Directors

Point-of-Contact: Office of Security, Security Management Division, OPSEC.TSA@dhs.gov, 571-227-2415 (Security Control Point) or 571-227-1946 (Office of Security fax)