Canonical ID: 08STATE48120_a
Subject: RESOURCE GUIDE FOR USG TERRORIST INFORMATION SHARING EFFORTS AND FOREIGN BORDER SCREENING PRACTICES
From: Secretary of State
To: Department of Homeland Security, Department of Justice, Federal Bureau of Investigation, Group Destinations All American Diplomatic Posts, Libya Tripoli, National Counterterrorism Center (NCTC), United States Customs Service
Original Classification: UNCLASSIFIED, FOR OFFICIAL USE ONLY
Current Classification: UNCLASSIFIED, FOR OFFICIAL USE ONLY
Previous Handling Restrictions: -- Not Assigned --
Archive Status: -- Not Assigned --
Type: TE
Locator: TEXT ONLINE
Reference(s): -- N/A or Blank --
Executive Order (E.O.): -- Not Assigned --
Markings: -- Not Assigned --
Enclosure: -- Not Assigned --
Concepts: -- Not Assigned --
TAGS: Consular Affairs--Consular Administration and Management [CMGT]
Consular Affairs--Visas [CVIS]
Political Affairs--Terrorists and Terrorism [PTER]
Office: -- N/A or Blank --
Document Character Count: 19159
Date: 2008 May 6, 22:52 (Tuesday)

UNCLAS SECTION 01 OF 05 STATE 048120

SENSITIVE
SIPDIS

E.O. 12958: N/A
TAGS: CVIS, CMGT, PTER, KLHS
SUBJECT: RESOURCE GUIDE FOR USG TERRORIST INFORMATION SHARING EFFORTS AND FOREIGN BORDER SCREENING PRACTICES

REF: A) 07 STATE 133921; B) 06 STATE 190832; C) 06

STATE 114591

1. (U) This is an action request, please see para 14.

2. (SBU) BACKGROUND: As a result of several different Homeland Security Presidential Directives (HSPDs) as well as 9/11 Commission Act requirements designed to enhance U.S. security, Washington agencies have concluded a number of biographic and biometric data exchange and information sharing agreements, both formal and informal, with foreign partners. These efforts are important tools in fighting terrorist travel and transnational crime, and often provide reciprocal benefits in the form of enhanced security for both the U.S. and host governments. However,

these sometimes overlapping efforts to facilitate information sharing have resulted in confusion at some posts. In order to improve transparency and coordination and to reduce confusion, the Office of the Coordinator for Counterterroism (S/CT) has outlined various interagency terrorist biographic and biometric information sharing agreement efforts and provided Washington points-of-contact, below.

3. (SBU) To coordinate these efforts, the Department chairs a number of interagency working groups (IWG) and intradepartmental efforts -- including the S/CT-chaired Departmental Homeland Security Coordinating Committee (HSCC), Bureua of Consular Affairs-chaired HSPD-6 IWG, and Information Sharing Environment (ISE) Foreign Partner Group, among others. The HSCC includes representatives from more than 20 of the Department's regional and functional bureaus and coordinates homeland security issues that impact the conduct of U.S. foreign policy and the work of the Department (Ref C). Posts are encouraged to utilize HSCC resources in identifying appropriate Department points-of-contact on a number of major international homeland security-related initiatives and are invited to visit the HSCC website on Intellipedia: http://www.intelink.sgov.gov/wiki/Portal:Coun terterror ism/Tab_3 . END BACKGROUND.

FOREIGN BORDER CONTROLS-- INFORMATION RESOURCE

4. (SBU) S/CT is pleased to announce that Foreign Border Information Collection, Screening, and Information Sharing Practices survey data also is now available as a resource on Intellipedia. Per reftels, in 2006-07, S/CT, in cooperation with the National Counterterrorism Center (NCTC), developed a survey soliciting information on country watchlist information, foreign entry/exit information collection, screening software in use at foreign ports of entry, and potential for concluding information sharing agreements. We appreciate posts' detailed and informative responses to the border control surveys, which have provided information of high value to analysts in identifying deficiencies in national screening systems frequently exploited by terrorists for travel. S/CT has consolidated responses and posted a matrix to its Intellipedia site as a tool for posts, the intelligence community, foreign assistance planners, and other experts to target deficiencies in foreign partner's border screening systems. We already have collected data from over 120 countries and will continue to update this matrix as additional information and updates are received. Visit the portal at: http://www.intelink.sgov.gov/wiki/Foreign_Bor der_Contr ols_Information_Sharing_Surveys .

TERRORIST INFORMATION SHARING AGREEMENTS

5. (SBU) In order to improve transparency and coordination, Department also has consolidated various interagency terrorist information sharing initiatives below and provided Washington points-of-contact. Close coordination between Washington stakeholders and post personnel is vital to ensuring the success of these efforts.

STATE 00048120 002 OF 005

Homeland Security Presidential Directive 6 (HSPD-6)
---

6. (SBU) HSPD-6 directed the Secretary of State to lead the USG effort to share terrorist screening information with foreign partners beginning with countries participating in the Visa Waiver Program (VWP)(see below). This directive stems from recommendations made by the 9/11 Commission, and its implementation is a high priority for the Bureau of Consular Affairs (CA), which is leading this effort for the Department. CA co-chairs an Interagency Working Group with the HSC, and is partnered operationally with the Terrorist Screening Center. HSPD-6 agreements enable reciprocal exchange of information about known and suspected terrorists, establish protocols for managing encounters with watchlisted individuals, and are designed to augment existing informal information sharing arrangements between immigration, law enforcement, and intelligence agencies. Consuls General and chiefs from other sections at posts have contributed greatly to the success experienced to date. Conclusion of an HSPD-6 agreement will be required for VWP aspirants prior to their designation in the program.

POC: DOS/CA/P/IP Division Chief Alcy Frelick (FrelickAR@state.gov; (202) 663-1633); DOS/CA/P/IP Deputy Director Peter Thompson (ThompsonPM@state.gov; (202) 663-1635).

Advance Passenger Information System (APIS)
---

7. (SBU) APIS is a regulatory requirement imposed by the United States and many other governments in which air carriers must submit biographic data on air passengers, crew members, and non-crew members for the

purpose of border screening. API generally consists of information that appears on the biographical data page of official travel documents, such as passports. Each air carrier, foreign and domestic, operating a passenger flight to/from the U.S. must electronically transmit to Department of Homeland Security/U.S. Customs and Border Protection (DHS/CBP) a passenger and crew manifest in advance of departure. Information forwarded to CBP is used by the National Targeting Center (NTC) for screening against lookout data in law enforcement and terrorist databases held by different USG agencies. Advanced screening of API forms the basis of our ability to identify potential threats before they arrive at U.S. ports of entry. Through existing relationships with some countries, DHS may obtain API for flights between a partner nation and 3rd countries. Through this model, DHS is able to promote improved border security in locations where individuals may then transit to the U.S., acquire additional information in support of DHS border management activities, and collect intelligence on the movements of individuals who are the subject of USG lookouts. DHS remains interested in striking similar arrangements with willing partners. Washington agencies are very interested in reporting on the development of API or similar programs in other nations for the purposes of ensuring compatible regulatory and operational approaches.

POC: DHS/Office of International Affairs Michael Scardaville; (Mike.Scardaville@dhs.gov, (202) 282-8321); DOS/EEB/TRA John Emery (EmeryJB@state.gov; (202) 647-9470)

Passenger Name Record (PNR) Data
---

8. (SBU) Also collected and transmitted by carriers, PNR is similar in objective to the API program in that it allows for the electronic transmission of data on air passengers and crew. However, PNR data is broader in scope than the biographic data captured under API as it contains information from the computer reservation system (such as Sabre or Worldspan) for a

passenger or group of passengers traveling together. PNR provides significant additional passenger information including ticketing details, itineraries, destination address, embarkation point, and PNR locator code number. Carriers are required to make available to CBP PNR for all flights to/from the U.S.

This information is invaluable in identifying linkages between passengers as well as identifying high risk travelers for whom biographic data is not held in a lookout. The perceived sensitive nature of PNR information among privacy advocates has resulted in the negotiation of data security and privacy safeguards between the U.S., the European Union, and Switzerland. Supported by the Department, DHS is also attempting to secure commitments from selected governments to obtain PNR for routes lacking a U.S. nexus. As with API, Washington agencies remain interested in reporting on the development of similar programs in other nations.

POC: DHS/Office of International Affairs Michael Scardaville; (Mike.Scardaville@dhs.gov, (202) 282-8321); DOS/EEB/TRA John Emery (EmeryJB@state.gov; (202) 647-9470)

Visa Waiver Program (VWP)
---

9. (SBU) The VWP enables eligible nationals of participating countries to travel to the U.S. for stays of 90 days or less without obtaining a visa. The program was initially designed to facilitate travel, promote domestic economic prosperity, and allow Department resources to be devoted to countries with higher refusal and overstay rates. VWP travelers are currently screened through APIS and PNR prior to admission to the U.S. and are enrolled in DHS's US-VISIT program (see below) at the port of entry. Currently 27 countries participate in the program. Both the current participating countries and countries seeking to join the VWP will have to comply with new security enhancements mandated by the 9/11 Commission Act -- including passenger information sharing, more timely reporting of both blank and issued lost and stolen passports, and use of the ESTA system (see below) to be created. DHS has formalized requirements for VWP participation into a non-binding Memorandum of Understanding (MOU) and associated implementing arrangements that each member and aspirant country will be required to sign. As of April 2008, DHS has signed VWP MOUs with eight countries: Czech Republic, Estonia, Hungary, South Korea, Latvia, Lithuania, Malta, and Slovakia.

POC: DHS/VWP Director Marc Frey (marc.frey@dhs.gov; (202)-282-9555); DOS/CA/VO/F Director John Brennan (BrennanJB@state.gov; (202)663-1160)

Electronic System of Travel Authorization (ESTA)

---

10. (SBU) The establishment of an ESTA for VWP countries and aspirants is a requirement under the 9/11 Act of 2007. The ESTA will collect basic passenger biographic information similar to that contained on the Nonimmigrant Alien Arrival/Departure (I-94W) form. CBP is developing the ESTA as a web-based application and screening mechanism for direct access by VWP travelers. Applications will be screened against U.S. watchlists. To the extent possible, ESTA is projected to provide quick determinations of eligibility for individuals to travel under the VWP. However, a positive determination will not connote admissibility into the U.S. If an ESTA application is not approved, a message will refer the applicant to the local embassy or consulate to apply for a non-immigrant visa to travel to the U.S. DHS is seeking to initiate an operational ESTA system during summer 2008 and will partner closely with the Department and U.S. embassies and consulates worldwide to ensure a smooth rollout and effective public awareness effort.

POC: DHS/Policy Justin Matthes

STATE 00048120 004 OF 005

(justin.matthes1@dhs.gov); DOS/CA/VO/F Director John Brennan (BrennanJB@state.gov; (202)663-1160)

TIP/PISCES
---

11. (SBU) The Terrorist Interdiction Program (TIP) seeks to constrain terrorist mobility globally by helping other countries at risk of terrorist activity enhance their border security capabilities. TIP provides countries with a computerized watchlisting system known as PISCES (Personal Identification Secure Comparison and Evaluation System). Countries are identified for eligibility to participate in TIP based on known terrorist activity or transit patterns, need for a watchlisting system, and political will to cooperate. TIP installs PISCES hardware and software at selected points of entry, including international airports and major border crossings. The system enables host nation border control officials to identify suspect travelers against a current watchlist and has integrated capability for both biographic and biometric data capture. PISCES is installed at both arrival and departure terminals so that host officials can identify travelers entering and exiting the

country. PISCES also enables immigration officials to use the system to collect, compare, and analyze data for investigative purposes. TIP/PISCES is currently operational in the following countries: Afghanistan, Cambodia, Cote d'Ivoire, Djibouti, Ethiopia, Ghana, Iraq, Kenya, Kosovo, Macedonia, Malta, Nepal, Pakistan, Tanzania, Thailand, Yemen, and Zambia.

POC: DOS/S/CT Ken McKune (McKuneKR@state.gov; (202) 647-6718)

Integrated Automated Fingerprint Identification System (IAFIS)

---

12. (SBU) IAFIS is a biometric identification system that uses digital imaging technology to obtain, store, and analyze fingerprint data. Administered by the Federal Bureau of Investigation (FBI), IAFIS is a mature technology which has been proven highly effective in identification management and fraud prevention and is accepted in courts of law. With over 55 million records, the IAFIS is the most comprehensive criminal fingerprint database in the world. In an effort to continue to expand the data, FBI's Criminal Justice Information Services (CJIS) Global Initiatives Unit (GIU) seeks to conclude fingerprint data transfers with foreign governments. These transfers often are concluded informally -- although formal agreements also may be negotiated. Under the program, foreign governments provide fingerprint records to add to the IAFIS database and in return can request specific information from the U.S. database through a case-by-case query mechanism, often through the LEGAT at post. CJIS already has facilitated a number of data transfers including several from Western Hemisphere countries. Consular sections capture ten-digit fingerprint scans routinely from most visa applicants, which also are run against the IAFIS database; and DHS has the capability of screening US-VISIT biometrics captured at U.S. ports of entry through IAFIS.

POC: FBI/CJIS: Gary Wheeler (304)625-2604; GWheele4@Leo.Gov; DOS/CA/VO/I: John Cook (202) 261-8016; CookJG@state.gov

---

Visitor Immigrant Status Indicator Technology (US-VISIT) Program

---

13. (SBU) US-VISIT allows for the biometric screening of international travelers. The program captures and compares biometric data and biographic information collected from non-citizens at U.S. ports of entry against law enforcement, counterterrorism, and

immigration enforcement records as well as identity information collected at visa issuing posts and by DHS immigration authorities. It also captures biometric and biographic information on individuals traveling under the VWP at ports of entry in the U.S. By relying on biometrics, US-VISIT provides another means of identifying individuals who may be traveling under a fraudulent identity. For example, Consular officers overseas capture 10-digit fingerscans and photos of visa applicants; these are run against IDENT (the US-VISIT biometric database) and IAFIS. By verifying the fingerprints of arriving travelers, CBP officers are able to verify that the person presenting the visa is the same individual as the one issued the visa, reducing potential fraud associated with imposter travel, document alteration, or forgery. The program incorporates privacy and data protection provisions into its operations. With nearly 200 million records (primarily of non-U.S. Persons, lawful permanent residents (LPRs), and naturalized persons) and growing, US-VISIT has become the largest fingerprint database in the world. This fact has not escaped foreign government attention and in some cases, US-VISIT holds more fingerprint data of a given countries' citizens than that country itself. US-VISIT has concluded pilot data sharing agreements with Australia, Canada, and the United Kingdom to combat crime and terrorism as well as make immigration and border management systems more robust for individual travelers. In some cases, US-VISIT has assisted foreign terrorist investigations by linking a latent fingerprint found abroad to the digital photo, passport data, and fingerprints of a traveler who arrived in the U.S. US-VISIT's agreements also provide US-VISIT with additional useful information related to travelers (e.g. prior attempts to seek asylum in other countries, terrorist biometrics, etc). DHS, in coordination with the Department, may seek to conclude additional bilateral data exchange agreements as needed in the future. Reporting on the DHS proposal for biometric screening of foreign travelers as they depart the U.S. -- also required by the 9/11 Commission Act -- is available septel.

POC: DHS: Marianne Kilgor-Martz; DOS/CA/VO/I: John Cook (202) 261-8016; CookJG@state.gov

14. (SBU) Action Request: Department requests this information be promulgated among country teams and other appropriate working groups -- in particular Law Enforcement Working Groups. Given that information sharing agreement efforts often overlap, it is critical that agencies coordinate closely with the Department and posts and do not/not discuss biometrics or other information sharing with host governments without country team coordination. Identification of Washington POCs for these efforts and other intradepartmental coordinating groups, such as the HSCC, should assist in this effort. Recognizing that agency POC's likely will change -- including with summer rotations -- S/CT periodically will update contact information on these efforts via cable and the HSCC Intellipedia portal. Department appreciates posts' invaluable reporting on host government border control systems and strongly urges posts to continue reporting on host government progress in developing similar programs in this area. End Action Request.

15. (U) Minimize considered.
RICE