



Department of Justice

STATEMENT OF

**SHAWN A. BRAY
DIRECTOR
INTERPOL WASHINGTON**

BEFORE THE

**SUBCOMMITTEE ON BORDER AND MARITIME SECURITY
COMMITTEE ON HOMELAND SECURITY
UNITED STATES HOUSE OF REPRESENTATIVES**

ENTITLED

“PASSPORT FRAUD: AN INTERNATIONAL VULNERABILITY”

PRESENTED

APRIL 4, 2014

**Statement of
Shawn A. Bray
Director
INTERPOL Washington**

**Before the
Subcommittee on Border and Maritime Security
Committee on Homeland Security
United States House of Representatives**

**At a Hearing Entitled
“Passport Fraud: An International Vulnerability”**

**Presented
April 4, 2014**

Chairman Miller, Ranking Member Jackson Lee, and distinguished members of the Subcommittee, it is an honor to be here today to provide you with an overview of the INTERPOL Stolen/Lost Travel Document Database, or SLTD, and how INTERPOL Washington, the United States National Central Bureau, and its partner agencies utilize this international resource to combat transnational crime and terrorism.

Background

INTERPOL

The International Criminal Police Organization – INTERPOL – is the largest international police organization in the world. Its membership is comprised of the respective national police authorities of its 190 member countries, which participate on a voluntary basis.

INTERPOL is a world renowned brand in the international law enforcement community, but one that is often misunderstood by the public at large. Simply put, INTERPOL exists to ensure and promote the widest possible mutual assistance between the criminal police authorities of its member countries, and it seeks to “...establish and develop all institutions likely to contribute effectively to the prevention and suppression of ordinary law crimes.”¹ INTERPOL is both mindful of the differing national laws of its member countries and active in its protection of human rights.

INTERPOL National Central Bureaus

Under INTERPOL’s constitution, each member country is required to establish and maintain a “National Central Bureau”, or NCB, responsible for ensuring the “constant and active co-

¹ Article 2, Constitution of the International Criminal Police Organization - INTERPOL

operation” of the particular country.² An NCB serves as a critical link between the national law enforcement authorities of an INTERPOL member country, its foreign counterparts, and the INTERPOL General Secretariat.³ Except for certain general guidelines and conditions of membership in INTERPOL, the structure, placement, and operation of an NCB is entirely within the control and discretion of the respective member country.

INTERPOL Washington – The United States National Central Bureau

Located in Washington, D.C., INTERPOL Washington is the United States’ National Central Bureau (USNCB). Our agency is unique in that it is a component of the U.S. Department of Justice and co-managed with the Department of Homeland Security under a Memorandum of Understanding.⁴ INTERPOL Washington’s mission is well-defined by statute and regulation and includes facilitating international police cooperation; transmitting information of a criminal justice, humanitarian and other law enforcement related nature, and coordinating and integrating information in international criminal investigations.⁵ Staffed entirely by U.S. law enforcement agents, officers, and analysts, INTERPOL Washington provides the means for over 18,000 federal, state, local, and tribal law enforcement agencies in the U.S. to communicate and collaborate with police globally. Just to clarify any potential ambiguity, let me underscore that the USNCB is not a part of the INTERPOL organization. It is a U.S. Government agency that serves as the U.S. link to INTERPOL.

Sharing INTERPOL Information

Fundamental to INTERPOL are its core functions to provide its member countries with secure global police communication services and access to its operational data services and databases. This is achieved through an encrypted, virtual private network known as the “I-24/7” secure communications system. INTERPOL ensures the quality of its data and the efficiency with which it is processed by adhering to a transparent set of operating guidelines known as *INTERPOL’s Rules on the Processing of Data*, or RPD.

Under the RPD, NCBs may directly access INTERPOL’s Information System. This access permits an NCB to manage its data contained in the system; query INTERPOL’s databases; transmit messages; obtain and use INTERPOL Notices, and follow up on positive database query results. The RPD also allows NCBs to extend system access to their respective national authorities. In the U.S., INTERPOL Washington extends query access to INTERPOL’s investigative databases, which includes the Stolen/Lost Travel Documents Database, or SLTD, to all U.S. law enforcement, border protection, and consular authorities in support of their official duties.

² Ibid, Article 31

³ Ibid, Article 32

⁴ Memorandum of Understanding Between the U.S. Department of Homeland Security and the U.S. Department of Justice Pertaining to U.S. Membership in the International Criminal Police Organization (INTERPOL), Management of the INTERPOL – U.S. National Central Bureau, and Related Matters

⁵ 22 U.S.C. 263a; Title 28 CFR Subpart F-2 § 0.34

The Stolen/Lost Travel Document Database (SLTD)

Terrorist attacks over the last few decades gave rise to the realization that many of the perpetrators were known suspects who had been traveling internationally while concealing their identity through the use of false passports. To address this threat, INTERPOL conceived the idea of creating a technology that would allow the real-time verification of travel documents that had been reported lost, stolen, or revoked by their respective national issuing authorities.

Developed in 2000 as a database of blank passports that had been reported stolen, SLTD rapidly expanded to include travel documents reported as stolen from, or lost by, the bearer. Becoming fully operational in July 2002, SLTD has grown from housing less than 300,000 records to more than 40,000,000 records in 2014, searchable in real-time via fixed or mobile network database solutions. Using either solution, query results are available to authorized law enforcement and border security users in mere seconds.

The SLTD is one of the largest INTERPOL databases and it is considered among the world's primary tools for detecting stolen and lost travel documents in order to prevent illicit international travel and false personation by criminals and terrorists. Specifically, SLTD is a searchable repository of non-personal information drawn from passports, visas, and identity documents that have been reported stolen or lost by issuing authorities of INTERPOL member countries. It also includes information about stolen passport blanks and travel documents that have been revoked by an issuing national authority.

SLTD authorized users are able to query specific passport numbers against the database in support of investigative or border security functions. A positive "hit" against the database will return data elements about a suspect document that include the issuing country, document type, date of the theft or loss, and a limited amount of information related to the circumstances of the theft or loss, as provided by the INTERPOL reporting country. SLTD data does not include Personally Identifiable Information about passport holders, as defined under U.S. law, nor does the database provide access to information about *all* U.S. passports – only those that have been reported as stolen, lost, or revoked by issuing national authorities.

Only a member country's passport issuing authority, in coordination with its corresponding NCB, is authorized to enter and modify records in SLTD pertaining to the theft, loss, or revocation of its national travel documents. In the United States, the Department of State's Bureau of Consular Affairs is the designated source for lost, stolen, or revoked U.S. passport data submitted to SLTD through INTERPOL Washington. Currently, more than 3 million of the more than 40 million records contained in SLTD pertain to U.S. passports.

Although strongly encouraged by INTERPOL, participation in SLTD is voluntary on the part of INTERPOL member countries. While levels of participation vary on a country-by-country basis, the United States has embraced SLTD as a critical part of its strategy to combat illicit international travel and enhanced border security.

United States Utilization of SLTD

United States participation in SLTD is managed through our Operations and Command Center. Working 24/7/365, INTERPOL Washington partners with U.S. Customs and Border Protection (CBP) and the Department of State to make SLTD available for vetting against all inbound and outbound international travelers and visa applicants. With respect to international air travel, CBP receives Advance Passenger Information System (APIS) data from the carriers for those travelers inbound to and outbound from the United States. CBP queries the foreign travel document data it receives via APIS data against SLTD for any matches to the listed travel documents. As an additional security measure, INTERPOL Washington also makes available all INTERPOL Notices and lookouts for fugitives, persons of interest, missing persons, and career criminals to CBP and all U.S. law enforcement via DHS's TECS and the National Crime Information Center database administered by the FBI.

In the event of a hit, our command center staff immediately seeks to verify and resolve all matches against SLTD on foreign travel documents with our foreign partners. Conversely, command center staff also coordinates with our international counterparts to resolve cases involving matches on U.S. passports presented at foreign border control points and to coordinate the appropriate administrative or law enforcement action.

In 2013, U.S. law enforcement, border security, and consular authorities queried SLTD more than 238 million times through INTERPOL Washington, which accounted for approximately 30 percent of all queries conducted by authorities world-wide. Of the more than 25,000 hits against the database that occurred during that time, the overwhelming majority were resolved administratively. A small number of these hits, however, represented a serious, potentially criminal concern, and were referred to the appropriate law enforcement authority for further investigation and resolution.

For example, INTERPOL Madrid coordinated with INTERPOL Washington last year to prevent an imposter, a Gambian national using stolen or lost U.S. passport, from traveling to New York. Investigation revealed the passport had been issued less than 30 days earlier. The subject was denied entry to the U.S. and the passport was recovered by Spanish authorities for return to U.S. authorities. The matter was referred to Spanish authorities for further investigation.

In another example, INTERPOL Sofia intercepted an Iranian national, who was traveling on a stolen or lost U.S. passport and posing as a U.S. citizen. INTERPOL Washington coordinated with U.S. and Bulgarian authorities to determine the subject's true identity, which resulted in his arrest and the recovery of the passport.

In addition to the large scale, systematic screening of international travelers, SLTD may also be queried in support of an investigation or other official matter. Building upon our *Law Enforcement Information Sharing Strategy*, we have now extended the ability to query SLTD to all local, state, federal, and tribal law enforcement agencies through nationally available systems such as Nlets and N-DEx, the FBI's National Data Exchange.

Continuing Challenges

Notwithstanding the considerable progress that has been achieved since SLTD was first introduced, significant challenges remain in realizing its full potential. Of the INTERPOL member countries that participate in SLTD, many do not routinely contribute data on lost/stolen documents and fewer still regularly screen travel documents against the database. This participation varies on a country-by-country basis as a consequence of such factors as national policy; lack of connection or cooperation between law enforcement, issuing, and border control authorities, and capacity, i.e. cost of deployment and existing IT infrastructure.

The Way Forward

Just as the use of SLTD continues to grow, so too does INTERPOL's vision for detecting and deterring the illicit international travel of criminals and terrorists. Building upon I-24/7, its proven and highly adaptable global police communications network, INTERPOL is today implementing additional tools and services to assist law enforcement. Recently made operational, INTERPOL's TDAWN – Travel Documents Associated With Notices – enables law enforcement officers to identify wanted criminals that are subject to INTERPOL Notices when checking associated travel documents.

TDAWN, as well as other operational and forensic databases that now form the “INTERPOL Travel ID and Document Center”, hold promise to further enhance efforts to combat the illicit international travel that threatens our public safety, transportation, commerce, and national security. And, just as INTERPOL Washington has aggressively exploited the use of SLTD, we will continue to explore the potential applications of these new and promising capabilities.

Chairman Miller, Ranking Member Jackson Lee, distinguished members of the Subcommittee; I sincerely appreciate the opportunity to testify about this important program and our role in it. I would be happy to answer any questions you may have.