TESTIMONY OF

ALAN D. BERSIN

ASSISTANT SECRETARY FOR INTERNATIONAL AFFAIRS AND
CHIEF DIPLOMATIC OFFICER
OFFICE OF INTERNATIONAL AFFAIRS
U.S. DEPARTMENT OF HOMELAND SECURITY

AND

JOHN P. WAGNER

ACTING DEPUTY ASSISTANT COMMISSIONER
OFFICE OF FIELD OPERATIONS
U.S. CUSTOMS AND BORDER PROTECTION

BEFORE

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

PASSPORT FRAUD

APRIL 4, 2014

Introduction

Chairman Miller, Ranking Member Jackson Lee, and distinguished Members of the Subcommittee. Thank you for holding this important hearing today to discuss document security in the context of international air travel.

On March 9, the International Criminal Police Organization (INTERPOL) confirmed that two of the passports used by passengers to board Malaysia Airlines flight 370 had been recorded in its Stolen and Lost Travel Documents (SLTD) database. INTERPOL's Secretary General, Ron Noble, noted that very few countries systematically query the SLTD database for the purposes of verifying whether a passport has been reported as lost or stolen. INTERPOL has said that in 2013 travelers boarded flights more than a billion times without having their passport numbers checked against the SLTD database. This number does not include any flight to the United States, but it is striking nonetheless. Even more troubling is the poor rate at which countries outside the U.S. Visa Waiver Program (VWP) are contributing information on lost and stolen passports to the SLTD database.

At the moment, our thoughts and prayers are with the missing passengers and crew who were on Malaysia Airlines flight 370. DHS appreciates the opportunity to discuss the important steps that we—in coordination with our partners at the Department of State and the U.S. National Central Bureau (USNCB)—have taken to mitigate vulnerabilities associated with persons attempting to travel on lost or stolen passports, which has been highlighted by the recent tragedy, and to talk about the importance of information exchange to the homeland security enterprise.

The Stolen and Lost Travel Document Database

INTERPOL is the world's largest international police organization with 190 member countries today. INTERPOL's primary goal is to ensure that police around the world have access to the tools and services necessary to do their jobs effectively. Among the services INTERPOL provides to the law enforcement entities of every member country is access to the SLTD database. The SLTD database is maintained by INTERPOL, and it contains over 40 million records provided by nearly 170 of the organization's members.

It is important to note that when an individual seeking admission to the United States, presents a passport, whether by land from Canada or Mexico, by commercial air, or by sea on a cruise ship, that passport is screened against the SLTD database prior to admission—in fact in many cases, they are screened against the database on multiple occasions. Unfortunately, most countries in the INTERPOL community do not screen travelers against the SLTD database as thoroughly as we do in the United States. The ability to screen travel information in advance – be it against the SLTD database or a national watchlist that included, for example, terrorist information – is an important element of effective border and transportation security.

More disturbing is the alarming number of countries that report very little—and in some cases no—lost and stolen passport data to INTERPOL for inclusion in the SLTD database. As a condition for participation, VWP countries are required to provide lost and stolen passport data to INTERPOL for inclusion in the SLTD database or to make such data available to the United States through other means as designated by the Secretary, and DHS continuously monitors that data to ensure compliance by our partners. The United States, Canada, and Europe, as well as our other VWP partners have provided the vast majority of the 40 million records in the SLTD database.

Alarmingly, some of the most populous countries in the world including China, India, and Indonesia, have contributed few—if any—records to the SLTD database. Despite the incredible development of the SLTD database since its inception following the September 11th attacks—40 million records added in the past twelve years is a truly noteworthy accomplishment—the lack of data provided by many INTERPOL member countries remains significant.

We firmly believe, based on DHS's operational experience since 9/11, that the automated and depersonalized screening of traveler data against derogatory administrative, counter terrorism, and law enforcement records is an essential part of the future for homeland security efforts around the world. The INTERPOL SLTD database is the quintessential example of one way countries can collaborate in preventing fraud and subsequent criminal activity. There is no reason why a passport should not be scanned every time an individual boards a plane to verify that the document provided is valid. These sorts of queries can be done almost instantaneously, occur completely automatically, and provide a first indicator of suspicion that can guide a law enforcement response in concert with the relevant passport issuing authority. The process provides significant confidence in the legitimacy of the document (assuming of course that the participating countries properly and accurately report their data into the SLTD database).

How the United States Uses SLTD

U.S. Customs and Border Protection (CBP) uses the SLTD database and data from the Department of State's (DOS's) Consular Lost and Stolen Passport (CLASP) and the Consular Visa Lookout and Support System (CLASS) in the air, land, and sea environments to verify the validity of both U.S. and foreign passports. For VWP travelers, CBP vets all Electronic System

for Travel Authorization applications against the SLTD database. In the land environment, when a traveler arrives at a land border port of entry, CBP officers will query the document in TECS[1], which includes Lost and Stolen U.S. Passports and the INTERPOL SLTD for foreign passports. If CBP receives a hit, it refers the individual to secondary inspection for questioning. During the secondary inspection, CBP determines if the individual is a mala fide traveler or if the individual is the true bearer of the reported lost or stolen passport.

In the air and sea environments, when CBP receives inbound and outbound carrier advance passenger information system (APIS) data for travelers with a foreign passport, it queries the INTERPOL SLTD database for any matches to the document type – passport, number and issuing country. For U.S. citizens utilizing U.S. passports, CBP queries TECS for matches to lost, stolen, and revoked U.S. Passports. In the air environment, if CBP detects lost, stolen, or revoked passports prior to boarding through CBP's pre-departure vetting or through the Immigration Advisory Program (IAP), CBP would make a recommendation to the air carrier not to board the passenger. If CBP notified the carrier, but the traveler was still allowed to board with the document that was the subject of a lost or stolen passport lookout, the carrier would be subject to a fine for violation of Section 273(a)(1) of the Immigration and Nationality Act.

CBP has also developed the Carrier Liaison Program (CLP), which enhances border security to the airlines and their security companies by identifying improperly documented passengers destined to the United States. CLP training enables participants, including airline check-in personnel, boarding agents, and security company staff, to receive hands-on instruction

[1] TECS (no longer an acronym) is a key border enforcement system supporting the vetting of travelers entering the United States and the requirements of other federal agencies used for law enforcement and immigration benefit purposes. TECS supports the sharing of information about people who are inadmissible or may pose a threat to the security of the United States through the creation and query of "lookout records." TECS is used by more than 70,000 users, including users from more than 20 federal agencies that use TECS in furtherance of their missions. TECS receives and processes traveler manifests from carriers and supports primary and secondary inspections for almost a million travelers and almost half a million vehicles at United States ports of entry each day.

in fraudulent document identification, passenger assessment, impostor identification, and traveler document verification. When carriers encounter a lost or stolen travel document, CLP training instructs the carriers to contact CBP's Regional Carrier Liaison Groups (RCLGs). The RCLG offices are 24/7 operations maintained at the airports in New York, Miami, and Honolulu, with each RCLG maintaining responsibility for specific areas of the world to respond to carrier concerns. The RCLGs will respond in real-time to carrier inquiries concerning the validity of travel documented presented. After an RCLG determination of the lost/stolen travel document has been made, the RCLG will make a recommendation to board the passenger or to deny boarding. To date, the CLP has trained 33,600 airline and security personnel.

INTERPOL and Information Sharing

The I-24/7 global police communications system, which our colleague Mr. Shawn Bray, the Director of the USNCB, can speak to at great length, is a marvel in today's world, and it is one that has largely gone unnoticed. Each of INTERPOL's 190 member countries has a National Central Bureau (NCB) that is typically housed within that country's national police agency. And most significantly, each of these NCBs is connected to the I-24/7 secure communications system. By using the INTERPOL network, the U.S. law enforcement community can exchange information in real-time and in a secure manner with our police counterparts in every other INTERPOL member country around the world. This is an exceptional capability, and we have only begun to tap the potential it embodies.

To be sure, there are real and current challenges to this vision. Despite the fact that DHS and the USNCB have worked to incorporate recommendations for data reporting and response times into INTERPOL's approved SLTD standard operating procedures, INTERPOL does not

require its member countries to implement them. With regard to screening passengers against the SLTD database, many countries do not have advance passenger information capabilities to screen travelers prior to arrival, or they have been unable to connect their immigration agencies to their NCBs in order to screen documents at the time of arrival. Many countries have been unable to connect their agencies that record lost or stolen passport information to their NCBs, so reporting that data has been a challenge. This may be due to a lack of the proper information technology systems within the country, internal restrictions on data-sharing between agencies, or simple bureaucratic complexity (for example, some countries record lost identity documents at local police stations). These are all best practices that we employ here in the United States that we shall continue to encourage our partner countries to adopt.

To help address these challenges among its member countries, INTERPOL—with assistance from DHS—has recently established the Integrated Border Management Task Force (IBMTF). The IBMTF is charged with assisting member countries in their approach to border management, and how to utilize the tools and services INTERPOL offers to that end. The project has included, for example, trainings for immigration officials on using the SLTD database to screen inbound passengers. The intent is to help member countries move toward more systematic approaches to the use of the SLTD database in daily operations. DHS remains supportive of INTERPOL's efforts in this regard.

INTERPOL understands, as we do at DHS, that sharing data on lost and stolen passports is an essential and fundamental part of protecting people against crime and terrorism. Whenever you are pulled over by state or local law enforcement, your driver's license is vetted to verify its validity and to determine any derogatory information for you. The SLTD database operates on the same principle, just on a global scale, and all countries should be encouraged to adopt similar

measures. INTERPOL's SLTD database provides them with that opportunity. It is already built, already in use, and the U.S. has already proven it is a reliable repository for lost and stolen passport data that can effectively be used during border screening. The task ahead is encouraging our partners to more fully utilize it, which will in turn only further add to its value.

Conclusion

DHS has instituted procedures to vet all U.S. inbound and outbound international travelers against the SLTD database. Any person with a travel document that has been reported lost or stolen to INTERPOL, who attempts to board a plane to or from the United States, will be denied boarding until he can verify his identity.

The ability to screen for lost or stolen travel documents, however, hinges upon foreign countries reporting their data to INTERPOL. This is why DHS has invested significantly in ensuring that all VWP countries report lost and stolen passports to INTERPOL, since the SLTD database is only as valuable as the data it contains.

DHS's engagement strategy going forward is based on "Three P's": Populate, Process, and Promote. We will continue to ensure that all VWP countries <u>populate</u> the SLTD database effectively, and we will emphasize to our other foreign partners the critical importance of populating the SLTD database with their lost and stolen passport data. We will work closely with INTERPOL to ensure that effective <u>processes</u> exist to coordinate an appropriate law enforcement response when a lost or stolen passport is encountered. Lastly, we will work bilaterally and multilaterally to <u>promote</u> effective use of the SLTD database based on DHS's experiences. As the "Three P's" are implemented, DHS hopes to be even more effective in

helping to secure the global aviation system, and U.S. citizens will have greater confidence in their safety abroad.

Thank you for the opportunity to testify today, for your continued support of the Department, and for your attention to this important issue. We would be pleased to answer any questions at this time.