SENATE JUDICIARY HEARING OF THE JUDICIARY COMMITTEE, SUBCOMMITTEE ON TERRORISM, TECHNOLOGY AND HOMELAND SECURITY
WASHINGTON DC, (USA)
2 MAY 2007

STATEMENT

BY

RONALD K. NOBLE
SECRETARY GENERAL
ICPO – INTERPOL

2 May 2007 – 10h00

US Senate Dirksen Building

Washington, D.C.

USA

Statement of Ronald K. Noble, Secretary General of Interpol

Before The Senate Judiciary Committee
Subcommittee on Terrorism, Technology, and Homeland Security

Interrupting Terrorist Travel: Strengthening the Security of International Travel Documents

2 May 2007

I. Terrorists Have Been Exploiting A Gaping Hole in Global Security Since At Least 1993

As the 9/11 Commission found -- "For terrorists, travel documents are as important as weapons. Terrorists must travel clandestinely to meet, train, plan, case targets, and gain access to attack."

On September 1, 1992 – almost 9 years to the day before the September 11 terrorist attacks on the US and the world – Ramzi Yousef, the convicted mastermind behind the first World Trade Center bombing in 1993, used a stolen blank Iraqi passport to reach the US where he claimed asylum upon his arrival. He flew here with co-conspirator Ahmad Ajaj, who possessed a stolen Swedish (visa waiver country) passport.

Almost a decade later, history repeated itself with the deadly terrorist September 11 attacks targeting the World Trade Center again and other vital US interests. According to the 9/11 Commission, two of the 9/11 hijackers entered the US using fraudulent passports, and six others may have also used fraudulent passports. Even with the heightened security following 9/11, there remain documented cases of foreigners entering the US using falsified stolen passports – including at least 20 cases involving passports that had been stolen (as part of a batch of 708 blank passports) in a city that was home to an al Qaeda cell that "played a significant role in providing financial and logistical support for September 11th terrorists." See DHS OIG-05-07 (December 2004).

Terrorist use of fraudulent travel documents was one of the most dangerous gaps in global security back around the time of September, 2001. Unfortunately, it still is today.

Indeed, even today – 5½ years after 9/11 – terrorists and other criminals can all too freely travel the world to plot and execute their attacks and commit other crimes, while concealing their identities through the use of fraudulent passports. Fraudulent passports have been used by, or found in the possession of, terrorists involved in recent attacks, including the 2004 Madrid bombing, and the 2005 London bombing (attacks that killed 243 people and injured over 2,400 others).

Terrorist use of fraudulent passports is the subject of two recent reports issued by the US Government Accountability Office, one issued on 7 September 2006 (GAO-06-1090T), and the other issued on January 24, 2007 (GAO-07-375). The 7 September 2006 GAO Report found that stolen and lost passports are "prized travel documents among terrorists" and "officials acknowledge that an undetermined number of inadmissible aliens may have entered the US using a lost or stolen passport." The 24 January 2007 GAO Report reiterated these findings.

Terrorists and other criminals know they can use falsified stolen passports with little chance of detection. Stolen passports, particularly those stolen in blank form, present the greatest threat because they can be made into fraudulent passports that are among the most difficult to detect.

A recent example will illustrate this.

On 20 January 2007, eleven individuals who had arrived on a flight from Spain were stopped at the Monterrey airport in Mexico, after a vigilant border officer became suspicious of their reasons for visiting Mexico. The ensuing investigation revealed that the 11 individuals were, in fact, Iraqis who had traveled from Iraq, through Turkey and Greece by land and sea, and then by air to Spain and Mexico, with the ultimate goal of crossing into the US illegally, allegedly to seek asylum – just like Ramzi Yousef in 1992.

Interpol later became involved, and discovered that the Cypriot passports that were used by 8 of the Iraqis were registered in Interpol's stolen travel document database as part of a lot of 850 passports that had been stolen in blank form in 2003. But the Mexican border security system is not connected to the Interpol database, so their immigration officers did not know this.

While preliminary investigations suggests that these eleven Iraqis do not appear to have been terrorists, this example illustrates, among other things, that those involved in the business of supplying fraudulent stolen passports to those who seek to travel under false identities know they can do so with little chance of detection. And they are right about this – there is little chance that the fraudulent passports will be detected in a systematic fashion throughout the world. Indeed, here we have a case where passports were stolen in 2003, and they were brazenly used years later in 2007, and the reason the users were not successful is because a border guard happen to become suspicious of their travel story.

There are many examples where people have used stolen passports to travel for terrorist or other criminal purposes. Wali Khan, convicted in the Manila airline bombing plot with Ramzi

Yousef, possessed a stolen Norwegian (visa waiver country) passport. Though Khan never traveled to the US, his case demonstrates the need for the US's vigilance to go beyond its borders in order for the US and its citizens to be protected from terrorist attacks. The planning and preparation of terrorist attacks targeting the US can and do occur all over the world.

Another example of the worldwide threat posed by stolen blank passports involves one of the chief suspects (Milorad Ulemek) currently on trial for the assassination of Serbian Prime Minister Zoran Dindic in 2003. Ulemek used a falsified stolen Croatian passport to travel extensively in allegedly planning and carrying out the assassination. After he was arrested, it was discovered that his fraudulent stolen passport had been stamped 26 times by law enforcement officers in 6 countries.

Another recent example involves a wanted War Criminal, Ante Gotovina, who was wanted for war crimes and crimes against humanity. He had no problems using a falsified stolen passport to travel through 16 countries throughout several years, making over 40 border crossings, before he was finally captured in 2005. He was captured based on an Interpol Red Notice, his falsified stolen passport having never been detected by law enforcement officers at the borders, when it easily could have been detected using Interpol's Stolen and Lost Travel Document database.

These examples reinforce the view that unless there is a systematic way for countries' law enforcement officers to determine whether passports have been reported stolen, all countries risk that more terrorists and other dangerous criminals will use them to travel the world freely in order to plan and perpetrate deadly attacks. Not just terrorists, but also other varieties of dangerous criminals regularly use fraudulent stolen passports to conceal their identities in order to travel internationally undetected, plan and commit crimes, and evade justice.

II. Interpol's Response: Creation of the Global Database of Stolen & Lost Travel Documents and the Technology to Connect it to Border Systems Worldwide

To address this threat, Interpol created a global database of stolen and lost travel documents (the SLTD database), as well as the technology needed to make this database accessible to officers around the world at airports, seaports, other border entry points, and, indeed, at any field location. This technology, which we call MIND/FIND, is revolutionizing the way countries conduct border security.

A. The Interpol SLTD Database

Recognizing that there was no single global repository of information on stolen and lost travel documents, Interpol launched its SLTD database in 2002. The database began with approximately 3,000 passports reported stolen from 10 countries. It has since grown astronomically to 14.4 million stolen and lost travel documents from 123 countries. This includes 6.7 million passports and 7.7 million other types of travel documents (identity cards, visas, etc.). Included within the passports are many that were stolen in blank form, which pose the greatest threat because they can be made into fraudulent passports that are among the most difficult to detect. Below is a sampling of some the blank passports in the SLTD database. (With 63 Interpol member countries still not reporting stolen or lost passports to Interpol, this list is obviously incomplete.)

Through Interpol's secure global police communication system (called I-24/7), which is deployed throughout 185 countries, officers can query the SLTD database and instantly determine whether a travel document has been reported to Interpol as stolen or lost. This access is available at the Interpol National Central Bureau (NCB) located in each country. Indeed, Interpol encourages all of its member countries to extend this access beyond their NCBs – to all of their law enforcement agencies (especially at points of entry), and a growing number of countries are doing so.

It should be noted that there are no privacy issues regarding the SLTD database, as it contains no personal information, such as the name, date of birth, or any other identifying information of the lawful bearer. Such information remains with the country that issued the passport. The purpose of Interpol's database is to permit the rapid and systematic identification of potential criminals and security risks. Once the initial identification has been made, the person is moved from primary to secondary inspection where the member countries can immediately engage in bi-lateral discussions to determine who the bearer of the passport that has been reported lost or stolen really is. If and when the consulting of Interpol's SLTD database occurs prior to the person's boarding of a flight, the bi-lateral country consultations can occur before the traveler reaches his or her final destination point.

As stated above, Interpol's SLTD database collects information related to the document itself (i.e., the number of the document, the type of document, the issuing country, and the date of the theft or loss), not to the bearer of the document. Interpol intentionally designed its database in this regard in order to avoid complaints that the personal data of innocent individuals would be made a part of Interpol's database. Interpol's approach has allowed its database to be populated with data from countries that otherwise would never haven been willing to share their data globally. This is a common thread to Interpol's philosophy. We try to find ways that encourage countries to share police information. Interpol's approach has proved valuable and successful.

To date, the Interpol SLTD database has been endorsed as an effective law enforcement tool by numerous regional Chiefs of Police networks throughout the world, and is strongly supported by numerous international organizations, including the United Nations Security Council, the G8,

the European Union, the Asia-Pacific Economic Cooperation (APEC), the Organization for Security and Cooperation in Europe (OSCE), and the International Civil Aviation Organization (ICAO). UN Security Council Resolution 1617 (2005) specifically urges countries "to ensure that stolen and lost passports and other travel documents are invalidated as soon as possible and share information on those documents with other member states through the Interpol database."

It is important to note at this point that Interpol respects the sovereignty of each member country as it relates to its SLTD database (and all Interpol databases). Only the sovereign country that issues the passport is authorized to enter, modify, or delete its own stolen and lost travel documents data in Interpol's database. The passport issuing country is the owner of such information. And the passport issuing country can place restrictions on which countries it will allow to see its data. These are important points to stress.

Interpol is not blind to the realities of the world in which we find ourselves. It will likely never be the case that all countries will wish to share all of their law enforcement related information with all other countries. Since the terrorists are continuously planning to kill and harm innocent people, Interpol tries to find flexible ways for countries that wish to share certain law enforcement information to do so. Taking the US as an example, it regularly chooses not to share law enforcement information with countries such as Syria, Iran, and Cuba – so Interpol's rules permit it to exclude those countries. Certain European countries give Interpol an itemized list of countries that can receive certain types of information, and not other types of information. It sounds complicated, and it is. But, Interpol has found that unless it respects a country's sovereign right to choose what to share and with whom to share it, a country will not be willing to share information.

Here are two examples that prove that even countries that are perceived as "enemies" can at times have common law enforcement goals: (1) The first country in the world to seek the arrest of Osama Bin Laden internationally for deadly terrorist attacks was Libya, at a time when Libya and the US had no formal diplomatic relations, and well before the deadly September 11 terrorist attacks (Libya did so via an Interpol international wanted person's notice – an Interpol Red Notice); (2) Ramzi Yousef (the convicted mastermind of the first World Trade Center attack) entered the US claiming asylum using a stolen Iraqi passport in 1992, when the US and Iraq were so-called enemies. These two examples make clear that it is against a country's own national security interest and safety to ignore law enforcement related information coming from a perceived "enemy." Instead, each country should make an independent determination about whether and how much to credit information coming from a perceived "enemy." Interpol's philosophy and way of working facilitates each and every member country's ability to do so.

B. The Interpol MIND/FIND Connection Technology

While usage of the SLTD database by NCBs and other law enforcement agencies may be helpful to investigators who want to check a specific suspicious travel document as part of a particular investigation, such usage will not prevent terrorists and other criminals from entering a country. In order to accomplish that, the SLTD database must be used by border control officers to screen passports at airports and other border entry points.

For example, in the case of Milorad Ulemek discussed above, the falsified stolen passport he used was one of 100 blank passports stolen from the Croatian Consulate in Mostar (Bosnia and Herzegovina) in April 1999, and the theft had been reported to Interpol. Although the SLTD database had not yet been created at the time of theft, it was already in place when Ulemek started travelling to plan for the crime with which he has been charged. Ulemek was never

stopped at any of his 26 border crossings because the passport was not checked against Interpol's SLTD database at those border entry points. Similarly, in the case of Ante Gotovina, the fraudulent stolen passport – which, incidentally, came from the same batch of 100 Croatian passports stolen in 1999 – which was used to travel throughout 16 countries was also listed in the Interpol SLTD database, but the subject countries were not checking passports against that database at their border entry points.

The fact is that Interpol's database was initially designed as an investigative tool, not as a border protection tool. The USNCB and US law enforcement should be credited with bringing this weakness to Interpol's attention. The USNCB consulted with the relevant US law enforcement entities to learn what they liked or disliked about Interpol's SLTD database. Based on this dialogue, Interpol learned that certain US law enforcement agencies complained that entering passport numbers manually at points of entry would be too time consuming.

This complaint led Interpol to re-conceive the purpose of its SLTD. Our member countries wanted a border control tool as well as an investigative tool. Without the US' support it would be virtually impossible to get global acceptance of its SLTD database as a valuable law enforcement tool. Without such acceptance, countries (including the US) would try to develop incomplete bi-lateral approaches to the problem of criminal use of stolen travel documents, which in Interpol's view, is the greatest threat to global security. Consequently, dedicated staff at Interpol's General Secretariat in Lyon, France developed technology that would allow law enforcement officers to instantly check Interpol's SLTD database at airports, seaports, other border entry points, and, indeed, at any field location.

Put another way, the honest and accurate feedback that we received (principally from US law enforcement) resulted in revolutionizing the way that border control can now be effectuated at points of entry throughout the world. While it is never pleasant to receive negative feedback, such feedback can provide great opportunities for change. Receiving and responding to such criticism in the past has helped make us a stronger and more relevant law enforcement organization in fighting terrorism and other forms of serious crime. Interpol is innovative and responsive to the needs of its 186 member countries.

To respond to these needs, Interpol developed technology that enables law enforcement to check Interpol's SLTD database at all border entry points. There are no extra steps – the same swipe of the passport automatically checks the Interpol database in parallel with the check of the national database. This technology (called MIND/FIND) has transformed the way that countries conduct border security.

The MIND/FIND technology refers to two different ways of connecting the SLTD database to border control systems. The choice is based on a country's technical infrastructure.

- The FIND system (which stands for Fixed Interpol Network Database) allows a country's national system to search Interpol's SLTD database in Lyon, France over the internet through a secure virtual private network (Interpol's I-24/7 global police communications system). When the passport is swiped, the system will check the Interpol SLTD database in parallel with the national database.

- The MIND system (which stands for Mobile Interpol Network Database) allows a country's national system to search a copy of the Interpol SLTD database that is located within the country. Interpol provides the country with an encrypted copy of the database on a storage device (called a MIND Box). When the passport is

swiped, the system will automatically check the Interpol SLTD database that is stored in the MIND Box in parallel with the national database. The copy of the database is automatically updated by Interpol, whenever the MIND Box is connected to Interpol through I-24/7. To prevent countries from using stale data, the Mind Boxes become inactive if not refreshed on-line within a certain number of days.

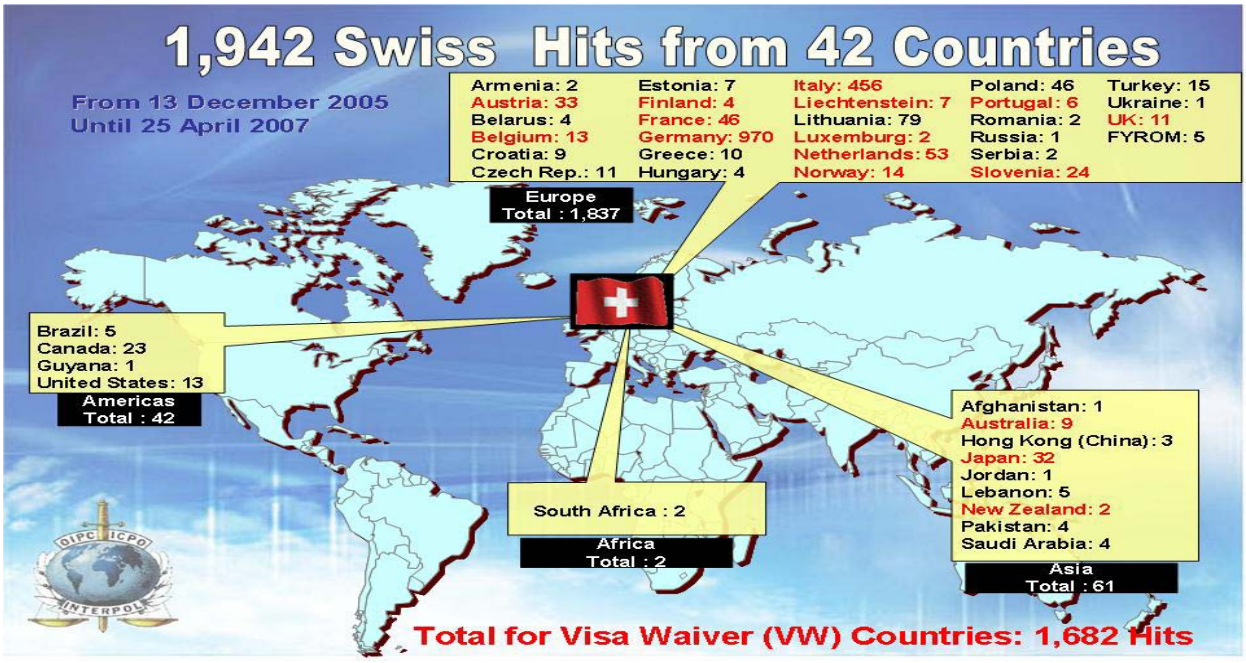
At present, MIND/FIND is used primarily to access the Interpol SLTD database and the Interpol Stolen Motor Vehicles (SMV) database, but work is underway to also include other databases.

C. MIND/FIND In Action

The MIND/FIND technology has dramatically changed the way countries conduct border security. This becomes clear when one compares the use and results of Interpol's SLTD database today with the use and results in 2003, the first full year in which the SLTD database was in operation. Thanks mainly to MIND/FIND, law enforcement officers now perform far more SLTD searches each and every day than in the entire year of 2003, and they obtain more hits each and every month than in the entire year of 2003.

1. Switzerland – The First Country to be Connected

On 13 December 2005, Switzerland became the first country to implement the MIND/FIND connection technology, enabling some 20,000 Swiss officers to screen passports at border entry points. Using this technology, Swiss officers conduct on the order of 300,000 to 400,000 database searches per month. And these searches get results – each month the Swiss detect over 100 persons attempting to enter their country using passports that had been reported stolen/lost.



The Swiss numbers bear witness to the urgent need for all countries to implement Interpol's MIND/FIND border security tool. A small, but growing number of countries are beginning to recognize this, but until every country actually implements this border security tool there will remain a dangerous gap in global security.

Based on the results achieved by Switzerland, other countries have expressed their interest in deploying the MIND/FIND connection technology to their border systems, and are in various stages of assessment, testing, or implementation. France, for example, began screening passports at Charles de Gaulle Airport in Paris on 8 June 2006. It has been conducting on the order of 140,000 searches per month, resulting in 18 "hits" a month. In April 2007, France extended the connection to 6 international train stations, 11 international seaports, and 21 airports.

Other countries, such as Algeria, Belgium, Bosnia and Herzegovina, Brazil, China, Croatia, Czech Republic, Denmark, Finland, Indonesia, Lithuania, Italy, Macedonia, Montenegro, New Zealand, Norway, Portugal, Saudi Arabia, Singapore, Spain, Turkey, the United Kingdom, and the United States, are in various stages of assessment, testing, or implementation of a MIND/FIND system.

The US has not yet begun screening passports against the Interpol SLTD database at its border entry points. The US has successfully tested the MIND/FIND system in order to ensure its functionality. DHS Secretary Michael Chertoff has stated that DHS has set a goal of being able to screen all passports against the Interpol SLTD database at all points of entry by the end of 2007.

2. The Caribbean – The First "Region" to be Connected

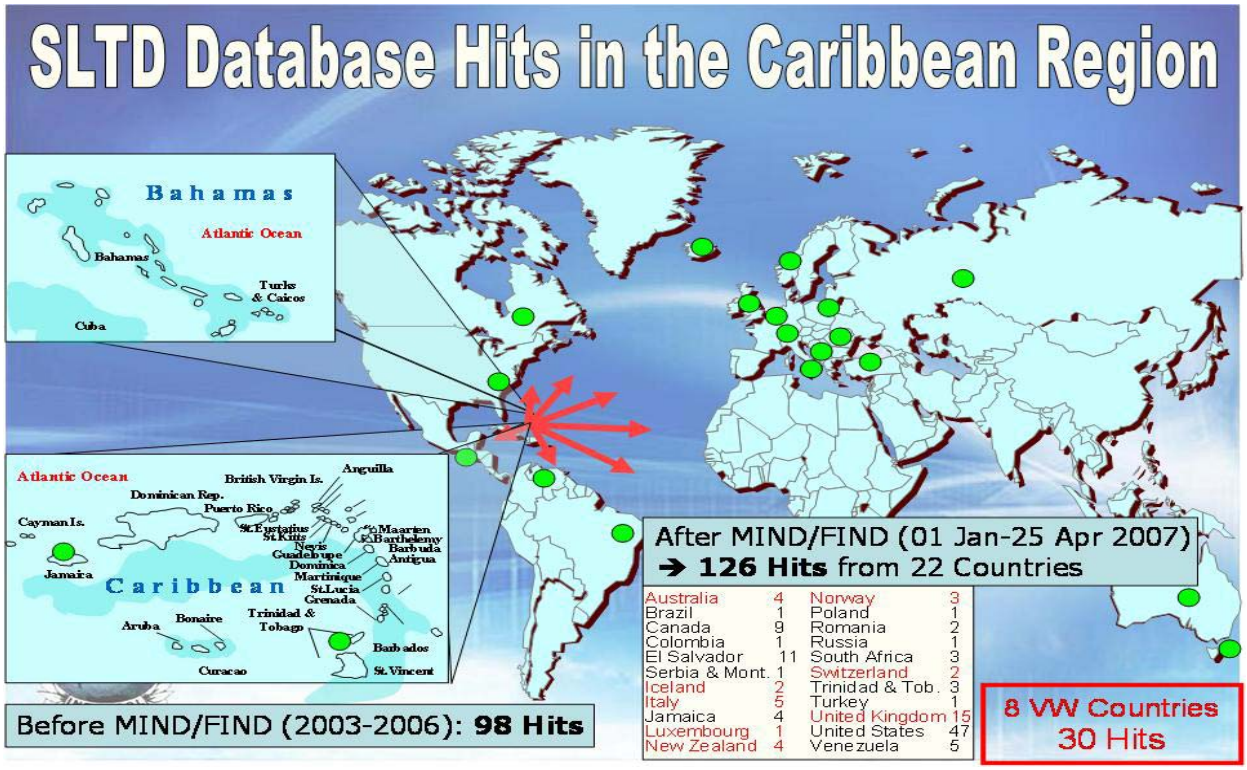
The Cricket World Cup was held in the Caribbean region from March through the end of April 2007. As Secretary General of Interpol, I took the decision to respond to the Caribbean's request for assistance in providing security for the Cricket World Cup – even though Interpol had no budgeted funds to do so, and even though I knew nothing about cricket. By consulting with Interpol member countries and doing a little reading, I learned that the Cricket World Cup is the 3d largest viewed sporting event in the world. It attracts millions of television spectators and some 100,000 visitors. It could have been a prized target for terrorists. And it is apparent that enhanced border security in that region enhances the security of the US (as the White House has observed through its "Third Border Initiative" that the Caribbean is often a gateway into the US), and it also enhances the security of every other country in the world.

The security issues were particularly challenging due to the fact that the games were hosted in multiple countries (nine in total) throughout the region. Despite its small size in terms of population, and despite the challenges of reaching agreement among so many sovereign nations, the Caribbean countries demonstrated the political will, the commitment, and the dedication to achieve what most of the world would have thought impossible. The Caribbean became the first region in the world to integrate a national and regional border control structure with Interpol's global SLTD. Some of these countries have even started performing advanced passenger manifest clearance procedures using Interpol's nominal database.

Thanks to the strong commitment of ministers, commissioners, chiefs of police, NCBs, and other members of the law enforcement community throughout the region and the world, all of the nine host countries (Barbados, Antigua & Barbuda, Grenada, St Kitts & Nevis, St Lucia, Trinidad & Tobago, St Vincent & The Grenadines, Guyana, and Jamaica) and two other countries in the region (Bahamas and Dominica) were able to screen passports against Interpol's SLTD database during the event, and can continue to do so now that the event is over.

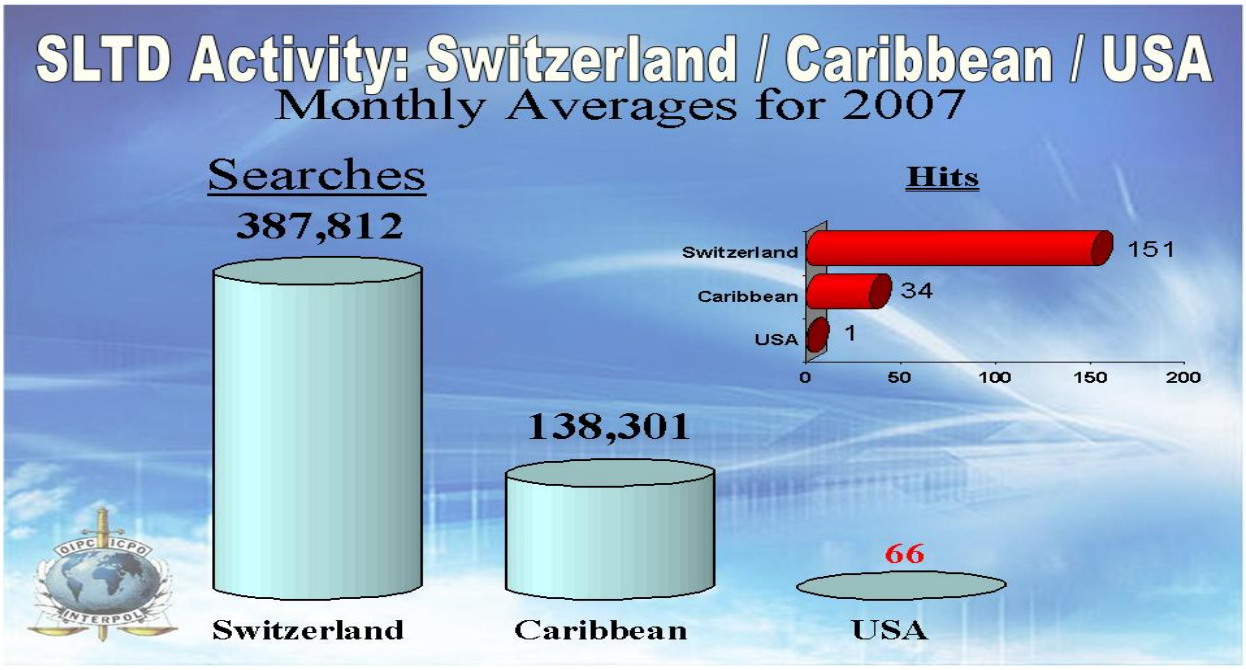
The results were nothing short of amazing, and are worthy of special recognition by the US and indeed all countries. While the total number of searches in Interpol's SLTD database by the

nine host countries amounted to just 1,218 searches in all the years prior to 2007, once the MIND/FIND system was running this number skyrocketed to 45,000 during the first month of 2007 alone. These searches led to 9 hits on passports that were reported stolen or lost. Through 25 April 2007, the Caribbean countries conducted nearly 500,000 searches, resulting in 126 hits.



Let us take a look behind one of those hits, in order to illustrate how the system actually enhances security in the Caribbean region. On 16 March 2007, immigration officers at the Barbados international airport checked a passport against Interpol's SLTD database, which resulted in a hit, indicating that the passport had been reported stolen or lost. The subject was interviewed and stated that the passport was his and that he had never reported it as stolen or lost. He further stated that he was a Nigerian by birth, but gained Venezuelan citizenship after living in Venezuela for seven years. After investigation, however, it was discovered that the passport was stolen, and the man was arrested.

Below is a graph showing the positive impact of the MIND/FIND technology on national law enforcement activity based on the MIND/FIND deployments in Switzerland and the Caribbean.



The significant difference in the activity levels is due to the fact that the SLTD database is now accessible through the MIND/FIND connection technology in Switzerland and the Caribbean, but not yet in the US.

Just this week Barbados' Deputy Prime Minister, Mia Mottley, requested additional staff from Interpol to ensure that the Caribbean's Joint Regional Command Center that was created for the Cricket World Cup could continue its fine work beyond this event. It wishes to continue the screening of passenger manifests against Interpol's global database as well as national and regional databases in the Caribbean. As has been made clear on a number of occasions, a more secure Caribbean region will lead to a more secure US. While Interpol may be able to provide temporary assistance to this initiative, the US can make the Caribbean's efforts more successful by supporting the Caribbean in ways that Interpol could never do on a long term basis. Doing so would benefit the Caribbean, the US, and the entire world's anti-terrorist and anti-crime efforts.

III. Implications For The Visa Waiver Program

The threat of terrorists and other criminals entering the US through the use of falsified stolen and lost travel documents is particularly acute in relation to the US Visa Waiver Program. As a recent GAO Report found, "lost and stolen passports from visa waiver countries are valuable travel documents for terrorists, criminals, and others who are seeking to hide their true identities to gain entry into the country." GAO-07-375 (January 24, 2007).

When people travel to the US using passports from visa waiver countries, they are not subject to the scrutiny of having to apply for and obtain a visa. This means that terrorists and other criminals know that if they buy passports that have been stolen or lost in these countries, then they can falsify those passports and use them to enter the US without being subject to any scrutiny from any US consulate. Consequently, such passports represent a particularly dangerous threat to US security. In fact, the 24 January 2007 GAO Report says that "experts consider it the greatest security problem posed by the Visa Waiver Program." And the facts on the ground bear this out.

Of the 288 database hits that the US obtained in 2006 by searching passports against the Interpol SLTD database, 140 were on travel documents from visa waiver countries (49% of the hits). For the same period (2006), of the 2,543 hits obtained by all the countries, 1,569 were on travel documents from visa waiver countries (62% of the hits).

To mitigate this danger, the 7 September 2006 GAO Report and the 24 January 2007 GAO Report recommend (i) the adoption of legislation that would require all visa waiver countries to provide the US and Interpol with data on all their stolen and lost passports, and (ii) the screening of all passports against Interpol's SLTD database at all points of entry.

These recommendations are the two main ingredients of an effective passport screening system. The database must have the stolen and lost travel document numbers, and passports must be screened against the database at border points of entry.

It should be noted again that there are no privacy issues regarding the SLTD database, as it contains no personal information. Only information relating to the document is stored in the database (document identification number, issuing country, type of document, whether it was stolen or lost in blank form, and any optional information regarding the theft/loss). And since a travel document does not belong to an individual, but is the property of the issuing country, there is no privacy issue with transmitting and storing this document related information.

It should also be noted that with respect to non-visa waiver countries, the US could significantly enhance its security by connecting the Department of State to the Interpol SLTD database, so that US consulates around the world could use this tool in assessing visa applications.

IV. Rolling out MIND/FIND Worldwide

The US and every other country has an interest in seeing that the MIND/FIND technology is implemented not just in their own country, but throughout the world. It has been recognized the world over that the defense of any one country begins beyond the border, not at the border. Rather than viewing one's border as the first line of defense, it should be viewed as the last line of defense. Interpol firmly believes that internal security is intrinsically linked to international security. Stopping terrorists outside the US can prevent them from appearing at the US' doorstep.

Let me say on the record at this point, that the US and the US Department of Homeland Security has an excellent and advanced network of border security tools, but no national system can really compare to a global system. If one were to draw a parallel to cars, one might say that the US has been building the American version of a Ferrari, while Interpol has been building a durable four-by-four. Keeping this simple parallel in mind will be very helpful to recognizing that the needs of the global community are at times different to the needs of any one nation.

National border control systems are necessarily based on internal information and bi-lateral agreements. Unfortunately, bilateral agreements do not offer any guarantees of completeness, and only offer a piecemeal solution to a problem that requires a comprehensive global approach.

By contrast, Interpol has a true and comprehensive system. An automated, global system. A system through which countries feed data directly into the database electronically, and update that data directly and electronically. And it allows border officers worldwide to screen travel documents against that database through connection technology we created, called MIND/FIND.

Unfortunately, wealthy countries sometimes forget that what works for them may not work for other countries. Interpol tries to find global systems that can complement national systems, whether they be advanced or basic. When wealthy countries see the benefits of such a dual, but complementary approach, what was previously thought impossible, becomes possible. The MIND/FIND connections in the Caribbean, for example were possible thanks to financial contributions from Canada.

The US endorsed the use of the SLTD database at border entry points around the world through the US' membership in the G-8, the UN, and ICAO. The world urgently needs this. It is my view that the US and the DHS need to take a leading role in encouraging and assisting countries in making this happen.

V. Checking Passports Before Passenger Arrival – Placing Additional Tripwires in the Paths of the Terrorists

The airline industry could also play a crucial role in helping to place additional tripwires in the paths of the terrorists – the more time we provide law enforcement between the moment suspicions are raised about an individual's passport and the moment that person shows up at the border, the safer our borders will be. This could be accomplished at a nominal cost and without any inconvenience to travelers. A system could be developed through which, before a plane's departure, the airline sends to Interpol the passport numbers of all the passengers, so that these passport numbers can be cheeked against Interpol's SLTD database, in order to inform relevant law enforcement whether any of the passengers are using any passports that had been reported stolen or lost. The airline would not be transmitting any personal information of the passengers, just the document numbers. If a document number is in the Interpol database, then relevant national law enforcement would be alerted. The control of travel documents in this manner would be non-discriminatory, non-intrusive, and raise no data protection issues. Moreover, since a travel document does not belong to an individual, but is the property of a country, there is no privacy issue with transmitting the document number.

If the travel document had been reported stolen or lost, a hit would be generated and seen by the police in the country that issued the passport, the police in the country from which the passenger is seeking to depart, and the countries to which the individual is travelling. Based on each country's own laws and procedures, the passenger could be detained before departure, so that the hit confirmation process could be conducted and appropriate action taken before departure, or the passenger could be allowed to travel while the hit confirmation process is conducted, and any necessary action could be taken upon arrival at the destination country. Interpol believes that this enhanced security control (which could be financed through a fee-based system) should be encouraged by the US and other countries.

VI. Conclusion – The World Needs A Truly Global and Comprehensive Border Control System

The recent example of the 11 Iraqis shows that there are organized criminal networks facilitating the illegal international travel of large groups of people. It also shows that US border security does not start in California, Texas, or in the immigration queue at US airports, but in Cyprus, Greece, or Spain. It is in every country's interest to see all the world's border controls strengthened. The organized criminal networks do not care to whom they sell, or for whom they customize stolen passports and travel documents. This problem is clearly global.

With this testimony, Interpol has tried to demonstrate that the gaping hole in global security that terrorists have been exploiting since the first World Trade Center attacks in 1993 might have gotten smaller on a national level, but is still unacceptably large at the global level. Interpol believes that the ability of terrorists to travel around the world based on fraudulent travel documents is the single greatest gap in global security.

Interpol also has tried to demonstrate that any one country's national or bi-lateral approach to border security is destined to fail. Each country works hard to secure its borders. Yet we all too often see, after a terrorist attack, that while the country had been doing a number of things well, there were gaps – gaps that were exploited by the terrorists to deadly effect.

To close this gap, the US and other countries have an interest in seeing that access to the Interpol global SLTD database is implemented, not just in their own country, but worldwide. If deployed throughout the world, we could finally turn towards the root of the problem, by acquiring a global view of the traffic in stolen and lost passports. At this point in time, no single police force in the world has a global overview of the extent of the problem. Widespread implementation of Interpol's MIND/FIND technology could change that and allow us to develop operational and strategic analysis on a global level.

But much more is needed from the entire world community to close this menacing global gap in border security. Let me draw another parallel. Look at the credit card industry and think about the resources that have been dedicated to ensuring that a secure global network is in place to protect the financial interests of the companies and the card holders. Billions of dollars are invested each year to ensure that trillions of dollars of transactions can take place securely. Card holders and criminals alike know that within minutes of reporting a credit card as stolen, the card's use can be canceled worldwide. It is not enough that the credit card is canceled in one country; it must be canceled in all countries for the issuing card company and for the card holder to be safe. The system works so well and so much is invested in maintaining the system that even unusual purchase patterns can be identified in time to permit instant verification that you are the legitimate cardholder. Why? To protect the financial interests and very existence of the card issuer, as well as to ensure that the global economy can function properly and continue to grow.

Now, take a look at passports. How many resources have been dedicated to ensure that the most precious and valuable national identity document (the passport) remains secure nationally and globally? How many citizens diligently stand in line removing their shoes, belts, clothing, baby formula, toothpaste and any other "suspicious" item because their governments tell them it is in their security interest to do so? What would these same citizens think if they knew that when they or others handed their passports at points of entry, these passports were not being screened against the world's only global database containing nearly 7 million stolen passports? They would be shocked. I know the answer to this question because I have traveled to over 100 countries as Interpol Secretary General, making this and other points about the urgent need to check global databases to ensure national security.

The question that keeps me up at night is this. If a terrorist attack occurs, and the terrorists used stolen travel documents, but those travel documents were not screened against Interpol's Global Stolen and Lost Travel Document database, what would we tell loved ones of those who were murdered? Could tell them that we did everything in our power to prevent it? Could we say that we were not aware of the risk? Could we say that we had other more important priorities? Could we say that we did not have a billion dollars to invest annually as a global community?

Let me close with the parallel that I used earlier because I do not want to be accused of using fear tactics to dramatize my point.

Let's continue to encourage countries to build Ferraris, for they serve a very useful purpose if you want to get somewhere really fast and you know the kind of road conditions that you will encounter. But, let's remember that if you did not know where you had to go really fast and if you did not know what road conditions you would encounter, would you pick a Ferrari or a four-by-four as your vehicle of choice?

In this epic anti-terrorist struggle in which we find ourselves, where terrorists and other dangerous criminals are trying to kill our citizens – often indiscriminately, we do not have the luxury of knowing where or under what conditions, we will encounter them. So, it is my firmly-held belief that we had better invest in building a dual, yet complementary, national and global border security system.