By Scott Stewart and Fred Burton

On June 1, 2009, the land and sea portion of the Western Hemisphere Travel Initiative (WHTI) will go into effect. The WHTI is a program launched as a result of the Intelligence Reform and Terrorism Prevention Act of 2004 and intended to standardize the documents required to enter the United States. The stated goal of WHTI is to facilitate entry for U.S. citizens and legitimate foreign visitors while reducing the possibility of people entering the country using fraudulent documents.

Prior to the WHTI, American travelers to Mexico, Canada and several countries in the Caribbean needed only a driver's license and birth certificate to re-enter the United States, while American travelers to other regions of the world required U.S. passports to return. This meant that immigration officials had to examine driver's licenses and birth certificates from every state, and since the driver's licenses and birth certificates of all the states change over time, there were literally hundreds of different types of documents that could be used by travelers at points of entry. In practical terms, this meant there was no way immigration officers could be familiar with the security features of each identification document, thereby making it easier for foreigners to use counterfeit or fraudulently altered documents to enter the country by claiming to be returning U.S. citizens.

The air portion of the WHTI went into effect in January 2007 and required that all international air travelers use passports to enter the United States. However, the land and sea implementation of WHTI will be a little different from the air portion. In addition to passports, travelers can also use U.S. passport cards (a driver's license-sized identification document), an enhanced driver's license (which are currently being issued by Michigan, New York, Vermont and Washington) or "special trusted" traveler identification cards such as Nexus and Sentri to enter the country by land or sea.

The WHTI will greatly simplify the number of travel documents that immigration officials have to scrutinize. It will also mean that the documents needed to enter the United States will be far harder to counterfeit, alter or obtain by fraud than the documents previously required for entry. This will make it more difficult for criminals, illegal aliens and militants to enter the United States, but it will by no means make it impossible.

An Evolutionary Process

Identity document fraud has existed for as long as identity documents have. Like much sophisticated crime, document fraud has been an evolutionary process. Advancements in document security have been followed by advancements in fraud techniques, which in turn have forced governments to continue to advance their security efforts. In recent years, the advent of color copiers, powerful desktop computers with sophisticated graphics programs and laser

printers has propelled this document-fraud arms race into overdrive.

In addition to sophisticated physical security features such as ultraviolet markings and holograms, perhaps the most significant security features of newer identification documents such as passports and visas are that they are machine-readable and linked to a database that can be cross-checked when the document is swiped through a reader at a point of entry. Since 2007, U.S. passports have also incorporated small contactless integrated circuits embedded in the back cover to securely store the information contained on the passport's photo page. These added security measures have limited the utility of completely counterfeit U.S. passports, which (for the most part) cannot be used to pass through a point of entry equipped with a reader connected to the central database. Such documents are used mostly for traveling abroad rather than for entering the United States.

Likewise, advancements in security features have also made it far more difficult to alter genuine documents by doing things like changing the photo affixed to it (referred to as a photo substitution or "photo sub"). Certainly, there are some very high-end document forgers who can still accomplish this — such as those employed by intelligence agencies — but such operations are very difficult and the documents produced are very expensive.

One of the benefits of the WHTI is that it will now force those wishing to obtain genuine documents by fraud to travel to a higher level — it has, in effect, upped the ante. As STRATFOR has long noted, driver's licenses pose serious national security vulnerability. Driver's licenses are, in fact, the closest thing to a U.S. national identity card. However, driver's licenses are issued by each state, and the process of getting one differs greatly from state to state. Criminals clearly have figured out how to work the system to get fraudulent driver's licenses. Some states make it easier to get licenses than others and people looking for fraudulent identification flock to those states. Within the states, there are also some department of motor vehicles (DMV) offices — and specific workers — known to be more lenient, and those seeking fraudulent licenses will intentionally visit those offices. In addition to corrupt DMV employees and states that issue driver's licenses to illegal immigrants, an illegal industry has arisen devoted entirely to producing counterfeit identification documents, compounding the problem.

Birth certificates are also relatively easy to obtain illegally. The relative ease of fraudulently obtaining birth certificates as well as driver's licenses is seen in federal document-fraud cases (both documents are required to apply for a U.S. passport). In a large majority of the passport-fraud cases worked by Diplomatic Security Service (DSS) special agents, the suspects have successfully obtained fraudulent driver's licenses and birth certificates, which are submitted in support of a passport application. It is not uncommon for DSS special agents to arrest suspects who possess multiple driver's licenses in different identities from the same state or even from different states. Such documents could have been used to travel across the U.S. border via land prior to the implementation of the WHTI.

Countermoves

For those able to afford the fees of high-end alien smugglers, who can charge up to $30,000 for

a package of identification documents that contains a genuine U.S. passport with genuine supporting documents (birth certificate, social security card and driver's license), or $10,000 to $15,000 for a genuine U.S. visa (tied to a database, the newer machine-readable visas are very difficult to counterfeit), the WHTI will not make much difference. These high-end document vendors obtain legitimate identification documents by paying corrupt officials who have been carefully cultivated.

That said, the WHTI should succeed in causing the vast majority of criminal aliens, illegal economic immigrants and even militants — people who have not traditionally patronized high-end document vendors — to change the way they enter the United States. Of course, perhaps the simplest way is to take the low road. That is, get to Canada or Mexico and then simply sneak across the border as an undocumented alien — something that hundreds of thousands of people do every year. Once inside the country, such aliens can link up with lower-level document vendors to obtain the driver's licenses, social security cards and other identity documents they need in order to live, work and travel around the country.

But there are other ways that the WHTI measures can be circumvented. For example, the crush of passport applications the WHTI is now causing will create a distinct vulnerability in the short term. Although the U.S. Department of State has hired a large number of new examiners to process the flood of passport applications it is receiving (and also a number of new DSS special agents to investigate fraud cases), the system is currently overwhelmed by the volume of passport applications.

Historically, passport examiners have had their performance evaluations based on the number of passport applications they process rather than on the number of fraudulent applications they catch (which has long been a source of friction between the DSS and the Bureau of Consular Affairs). This emphasis on numerical quotas has been documented in U.S. Government Accountability Office reports that have noted that the quotas essentially force examiners to take shortcuts in their fraud-detection efforts. As a result, many genuine passports have been issued to people who did not have a legitimate right to them. The current overwhelming flood of passport applications as a result of WHTI, when combined with a batch of new examiners who are rated on numerical quotas, will further enhance this vulnerability. Unless a passport application has an obvious fraud indicator, it will likely slip through the cracks and a fraudulent applicant will receive a genuine U.S. passport.

Stolen passports are another area to consider. In addition to being photo-subbed, which has become more difficult, stolen passports can also be used as travel documents by people who resemble the owner of the document. All the holograms, microprinting and other security features that have been placed on the laminates of passport photo pages tend to make it difficult to clearly see the photo of the passport holder. Also, people change over time, so a person who was issued a passport eight years ago can look substantially different from their passport photo today. The passport process and the laminate can also make it especially difficult to see the facial features of dark-skinned people. This means it is not at all uncommon for a person to be able to impersonate someone and use his or her passport without altering it. This problem persists, even with digital photos being included with the information embedded electronically in the memory chips of newer electronic passports.

Because of these possibilities, stolen passports are worth a tidy sum on the black market. Indeed, shortly after U.S. passports with green covers were issued, they were found to be extremely easy to photo-sub and were soon fetching $7,000 apiece on the black market in places like Jamaica and Haiti. In fact, criminal gangs quickly began offering tourists cash or drugs in exchange for the documents, and the criminal gangs would then turn around and sell them for a profit to document vendors. The problem of U.S. citizens selling their passports also persists today.

On the flip side, many Americans are unaware of the monetary value of their passport — which is several times the $100 they paid to have it issued. They do not realize that when they carry their passport it is like toting around a wad of $100 bills. Tour guides who collect the passports of all the people in their tour group and then keep them in a bag or backpack can end up carrying around tens of thousands of dollars in identification documents — which would make a really nice haul for a petty criminal in the Third World.

But U.S. passports are not the only ones at risk of being stolen. The changes in travel documents required to enter the United States will also place a premium on passports from countries that are included in the U.S. "visa waiver" program — that is, those countries whose citizens can travel to and remain in the United States for up to 90 days without a visa. There are currently 35 countries in the visa waiver program, including EU member states, Australia, Japan and a few others. The risk of theft is especially acute for those countries on the visa waiver list that issue passports that are easier to photo-sub than a U.S. passport. In some visa waiver countries, it is also cheaper and easier to obtain a genuine passport from a corrupt government official than it is in the United States.

While there are efforts currently under way to create an international database to rapidly share data about lost and stolen blank and issued passports, there is generally a time lag before lost and stolen foreign passports are entered into U.S. lookout systems. This lag provides ample time for someone to enter the United States on a photo-subbed passport, and it is not clear if retroactive searches are made once the United States is notified of a stolen passport in order to determine if that passport was used to enter the United States during the lag period. Of course, once a person is inside the United States, it is fairly easy to obtain identification documents in another identity and simply disappear.

There have also been cases of jihadist groups using the passports of militants from visa waiver countries who have died in order to move other operatives into the United States. On Sept. 1, 1992, Ahmed Ajaj and Abdul Basit (also known as Ramzi Yousef) arrived at New York's Kennedy Airport. The two men had boarded a flight in Karachi, Pakistan, using photo-subbed passports that had been acquired from deceased jihadists. Ajaj used a Swedish passport in the name Khurram Khan and Basit used a British passport in the name Mohamed Azan.

Ultimately, the WHTI will help close some significant loopholes — especially regarding the use of fraud-prone driver's licenses and birth certificates for international travel — but the program will not end all document fraud. Document vendors will continue to shift and adjust their efforts to adapt to the WHTI and exploit other vulnerabilities in the system.