S. HRG. 109–987

BORDER INSECURITY, TAKE TWO: FAKE IDs FOIL THE FIRST LINE OF DEFENSE

HEARING

BEFORE THE

COMMITTEE ON FINANCE
UNITED STATES SENATE

ONE HUNDRED NINTH CONGRESS

SECOND SESSION

AUGUST 2, 2006

Printed for the use of the Committee on Finance

U.S. GOVERNMENT PRINTING OFFICE
38–554—PDF WASHINGTON : 2006

For sale by the Superintendent of Documents, U.S. Government Printing Office
Internet: bookstore.gpo.gov Phone: toll free (866) 512–1800; DC area (202) 512–1800
Fax: (202) 512–2104 Mail: Stop IDCC, Washington, DC 20402–0001

COMMITTEE ON FINANCE

CHARLES E. GRASSLEY, Iowa, *Chairman*

ORRIN G. HATCH, Utah
TRENT LOTT, Mississippi
OLYMPIA J. SNOWE, Maine
JON KYL, Arizona
CRAIG THOMAS, Wyoming
RICK SANTORUM, Pennsylvania
BILL FRIST, Tennessee
GORDON SMITH, Oregon
JIM BUNNING, Kentucky
MIKE CRAPO, Idaho

MAX BAUCUS, Montana
JOHN D. ROCKEFELLER IV, West Virginia
KENT CONRAD, North Dakota
JAMES M. JEFFORDS (I), Vermont
JEFF BINGAMAN, New Mexico
JOHN F. KERRY, Massachusetts
BLANCHE L. LINCOLN, Arkansas
RON WYDEN, Oregon
CHARLES E. SCHUMER, New York

KOLAN DAVIS, *Staff Director and Chief Counsel*
RUSSELL SULLIVAN, *Democratic Staff Director*

CONTENTS

OPENING STATEMENTS

WITNESSES

ALPHABETICAL LISTING AND APPENDIX MATERIAL

COMMUNICATIONS

BORDER INSECURITY, TAKE TWO: FAKE IDs FOIL THE FIRST LINE OF DEFENSE

WEDNESDAY, AUGUST 2, 2006

U.S. SENATE,
COMMITTEE ON FINANCE,
Washington, DC.

The hearing was convened, pursuant to notice, at 10:15 a.m., in room SD–215, Dirksen Senate Office Building, Hon. Charles E. Grassley (chairman of the committee) presiding.

Present: Senator Bingaman.

OPENING STATEMENT OF HON. CHARLES E. GRASSLEY, A U.S. SENATOR FROM IOWA, CHAIRMAN, COMMITTEE ON FINANCE

The CHAIRMAN. Good morning, everybody.

It is a sad occasion for the Baucus family today, because Senator Baucus's nephew, Colonel Philip E. Baucus, paid the ultimate price for the defense of freedom in America in the war on terror Saturday, because he was a brave Marine, and lost his life there in Iraq.

I have had a chance to talk to Senator Baucus about it. Even though it is a nephew, Senator Baucus is very, very sad, and very sad for his brother as well. So we grieve with the Baucus family, and that is why he is not going to be here today, and we can all understand that. But I want him to know that my prayers are with him and his family.

Senator Baucus and I talked about this meeting previously. He always makes opening statements. His statement, I am going to put in the record for him.

[The prepared statement of Senator Baucus appears in the appendix.]

The CHAIRMAN. Today's hearing is entitled "Border Insecurity, Take Two." Our purpose is to follow up on a hearing that we had in the year 2003 to examine the security of our Nation's borders and find out whether the situation has improved.

At that hearing, the Government Accountability Office testified about how easy it was for investigators of their agency to create phony driver's licenses, and a lot of other documents, using a common personal computer. The Government Accountability Office then used those fake documents to enter the United States.

Now, it has been nearly 5 years since 9/11, and more than 3 years since we held that first hearing. Things should have gotten better by now, but today the Government Accountability Office testifies that its investigators did it again. They used the same phony documents and the same fake IDs to cross the U.S. border 18 more times, and they were not ever caught once.

Those Government Accountability Office investigators could have been known criminals, wanted fugitives, or even terrorists, but they were just somehow waved into our country. Frankly, it is hard to believe that there has been so little progress in plugging this gaping hole that we have in what ought to be a security fence.

Congress, I think, has tried to do its part. Since that hearing, we passed the Real ID Act to set Federal standards for driver's licenses. We passed the Western Hemisphere Travel Initiative to require that everyone crossing the border carry either a passport or some other document that establishes the identify of that person, and the citizenship of that person.

Less than 2 years after setting that deadline, now some people are even talking about just putting it off. So, how ready are we? Today, the purpose of this meeting is to get a progress report. But, more importantly, what is being done in the meantime? What could be done to improve our security?

Inspectors who work for the U.S. Customs and Border Protection are this Nation's first line of defense against criminals and terrorists coming to America. They should have the best tools and they should have the best technology available to help them catch people using suspect documents.

However, as we will learn today, some stores give their clerks better tools to catch under-aged drinkers. That sounds, of course, incredible, but it is true. We will hear testimony about how private industry is using technology to scan documents of all kinds and determine, in just a matter of seconds, whether they are looking at a real document or a fake document.

We will also hear how similar technology has been implemented in State Departments of Motor Vehicles to help them comply with the Real ID Act, and we will hear about how foreign countries—to name two, Chile and Singapore—have given inspectors these tools to help secure the borders of those sovereign nations.

If document verification technology works for the private sector, for State governments, and for foreign countries, there is no excuse for not using it to protect America's borders as well.

Yet, the Homeland Security Agency appears to have no plans to implement any new technologies beyond sitting back and waiting for the Real ID Act and the other bills that we passed to take effect.

About 741 million people have crossed our border since the Government Accountability Office's testimony at our last hearing 3 years ago, and about 300 million more people will be crossing before the other documentation is put in place, that documentation which will be implemented in 2008, assuming that it is implemented on time.

Until someone does something to address this problem, criminals and terrorists will know that our front door is wide open.

Now, a comment about our second panel, because it might be interpreted that this committee or the Senate is endorsing a certain product. I want to make it very clear that those witnesses on the second panel who are going to talk about private industry and the document verification technology that they sell, that they were invited to tell us what kinds of solutions are currently available. The fact that they are testifying should in no way be taken as an endorsement by the committee of any particular product.

We will now go to our witnesses. We have Mr. Gregory Kutz, Director, Office of Forensic Audits and Special Investigations at the Government Accountability Office, accompanied by John Cooney, Assistant Director; Mr. Jayson Ahern, Assistant Commissioner of Operations, Customs and Border Protection, Department of Homeland Security; and Mr. Michael Everitt, Unit Chief, Forensic Document Laboratory, Immigration and Customs Enforcement, Department of Homeland Security.

Your written testimonies will be included in the record, so we would ask you to take the time that we have allotted to summarize, if that is your wish.

So we will go in the order in which you were introduced. Mr. Kutz, first.

STATEMENT OF GREGORY KUTZ, DIRECTOR, OFFICE OF FORENSIC AUDITS AND SPECIAL INVESTIGATIONS, GOVERNMENT ACCOUNTABILITY OFFICE; ACCOMPANIED BY JOHN COONEY, ASSISTANT DIRECTOR, FSI, WASHINGTON, DC

Mr. KUTZ. Chairman Grassley and Senator Bingaman, thank you for the opportunity to discuss our undercover operation to test border security.

Our operation was done in response to your concern that counterfeit documents could be used to enter the United States from Canada and Mexico. My testimony has two parts. First, our 2006 border crossings, and second, our crossings in 2002 and 2003.

First, we tested nine land border crossings, five at the U.S.-Canadian border and four at the U.S.-Mexican border. The purpose of our operation was to test whether Customs and Border Protection inspectors could identify counterfeit documents.

We crossed the U.S.-Canadian border from New York, Michigan, Idaho, and Washington. We crossed the U.S.-Mexican border from California, Arizona, and Texas. Six of our crossings were done using rental cars, three were by foot.

As shown on the poster board, we conducted our operation using counterfeit driver's licenses and birth certificates. As you can see, our driver's licenses were from West Virginia and Virginia, and our birth certificates were from New York and West Virginia.

To create these bogus documents, we used software and information that were available to the public. We also used the same bogus name and identifiers for the West Virginia driver's license that we used for our 2002 operation.

The next poster board shows a genuine Virginia driver's license and our counterfeit license. Specifically, notice the hologram on the genuine driver's license which is missing from the counterfeit driver's license. Part of our test was to use a driver's license that could be identified as a counterfeit. We did not attempt to develop a more sophisticated driver's license.

During 2006, two investigators successfully entered the United States, each crossing from nine locations. CBP inspectors never questioned the validity of our counterfeit documents. Further, in both Texas and Arizona, inspectors did not ask our investigators for any identification.

Moving on to my second point. We found similar vulnerabilities for crossings we did in 2002 and 2003. Using counterfeit documents, we entered the United States from both Canada and Mexico. Our land crossings were done in California, Texas, New York, and in Washington.

In two instances, we successfully entered the United States by ferry. We were caught once entering New York in 2003. Specifically, our investigator was detained by CBP inspectors until he identified himself as a GAO employee.

This individual used the same documents later in 2003 to enter the United States from California and Texas. Although this individual had been entered into what is referred to as the TECS system after being caught entering New York, he was able to enter again later in 2003 because no name check was done.

We briefed CBP officials about the results of our test in June of 2006. They acknowledge that their inspectors cannot identify all forms of counterfeit documents at land border crossings.

Note that the Western Hemisphere Travel Initiative calls for the Secretary of DHS to improve border security through use of passports and other documents by January of 2008. Subsequent legislation could delay that until June of 2009.

In conclusion, CBP inspectors clearly do not have the tools available to identify counterfeit documents. From a security standpoint, the current system will always be vulnerable to individuals entering the United States using counterfeit documents. The challenge for our country will be to develop a system that provides us with a secure border, but does not impede commerce.

Mr. Chairman, this ends my statement. Special Agent Cooney and I look forward to your questions.

The CHAIRMAN. Thank you. I am sorry if I mispronounced your name.

Mr. KUTZ. That is all right.

[The prepared statement of Mr. Kutz appears in the appendix.]

The CHAIRMAN. Mr. Ahern?

STATEMENT OF JAYSON AHERN, ASSISTANT COMMISSIONER FOR OPERATIONS, CUSTOMS AND BORDER PROTECTION, DEPARTMENT OF HOMELAND SECURITY, WASHINGTON, DC

Mr. AHERN. Good morning. Thank you, Chairman Grassley and Senator Bingaman, for the opportunity to appear before the committee today to discuss the recent GAO investigation into the U.S. Customs and Border Protection's ability to detect counterfeit driver's licenses and birth certificates.

We welcome the lessons we learned from GAO about how to better secure our country. In this case, GAO had verified a vulnerability that CBP is well aware of, and that fraudulent documents provide a gap in our security, specifically, our CBP officers have difficulty in detecting counterfeit birth certificates and driver's licenses.

But what we are talking about here is larger than just two American GAO investigators using fraudulent driver's licenses to get back into the United States. What we are talking about is the need for standardized documentation that will be used at our borders, and, in my view, the sooner, the better, sir. The CBP very strongly supports standardized documents that will make us more effective at our job and make the borders of this country more secure.

Let me put, also, this reported vulnerability into better perspective. Each day, CBP officers process more than 870,000 people arriving at our Nation's 130 land borders. Unlike international air and sea travel, where we receive advanced information through passenger manifest information and most of the individuals travel with passports, we do not have that luxury at the land borders here in the United States.

So, consequently, our officers must verify the authenticity of more than 8,000 different types of documents from various counties, cities, States, as well as some foreign countries on the spot, within a matter of minutes, to identify the identity of the individual, and also their citizenship.

As the 9/11 Commission reported, security requirements governing travel to and from Canada, Mexico, and parts of the Caribbean should be treated as equivalent to the security requirements for travel to and from other parts of the world.

Congress recognized this important principle when it passed the Intelligence Reform and Terrorism Protection Act of 2004, which included what is commonly known today as the Western Hemisphere Travel Initiative, WHTI.

For the purposes of identification, it is estimated that more than 40 percent of U.S. citizens today crossing through our land border ports currently use passports. That means that under the current law, for 60 percent of individuals, all they are required to do under the current statute is just to make an oral declaration of their citizenship for entry back in the United States.

I again state that birth certificates and driver's licenses are not secure, they are not verifiable, and they do not adjudicate citizenship. It proves that an individual can operate a vehicle. It is not proof of citizenship and it is not an acceptable admissibility document; the same with the birth certificate.

As we certainly saw with this GAO test, they can be easily manufactured and obtained through fraud. The standardization for travel documents is a critical step in securing this country's borders. Currently, there are thousands of different documents, as I stated, that can be presented to our officers each day.

Standardization of these documents will also eliminate the time-consuming need for verifying and reviewing the host of these distinct, sometimes illegible and unverifiable birth certificates, and other identity documents.

The use of these standardized documents will enable automated reading and vetting of the information, which will also be essential to achieving the facilitation benefits of WHTI. Valuable time is wasted, when we are looking at accuracy, to try to verify these documents when we have to do manual entries that are required currently.

In the future, automated reading and vetting of identity documents will be an important tool for us to distinguish the small percentage of individuals coming into this country who pose a potential threat against the legitimate traveling public volume.

The people whom we deal with today also present an infrastructure problem. The capacity of our ports is challenged. As we begin to look at additional documents, we have to also manage the wait times at our ports of entry.

Otherwise, the economic vitality of our country could be impacted as we take a look at doing increased checks at the land borders, and we have to strike the appropriate balance between security and facilitation of legitimate trade.

One of the things we have done to address that is through expanding our Trusted Traveler programs: Free and Secure Trade (FAST), the NEXUS program, the SENTRI program. We have, now, over 225,000 individuals enrolled in these types of trusted programs. We need to continue to expand these types of programs, and we are doing so this week with an expansion in Hidalgo, TX.

Just to put into perspective also our officers today, I want to speak very positively about what they do to secure this country, because I do not want this committee or the public to think that our officers are not on the job, doing a very good job at identifying fraudulent documents coming into the country that are unacceptable admissibility documents.

Last year, we intercepted more than 84,000 fraudulent documents at our ports of entry. We denied admission to over 565,000 inadmissible aliens coming into this country, all the while seizing more than 800,000 pounds of narcotics, and we arrested more than 23,000 subjects, and 17,000 criminal aliens coming into this country.

It is important, as we look to move forward, that we continue to evaluate the test of the Government Accountability Office. I urge that we do move forward with the implementation of WHTI without delay.

Thank you very much.

The CHAIRMAN. Thank you, Mr. Ahern.

[The prepared statement of Mr. Ahern appears in the appendix.]

The CHAIRMAN. Now, Mr. Everitt?

STATEMENT OF MICHAEL EVERITT, UNIT CHIEF, FORENSIC DOCUMENT LABORATORY, IMMIGRATION AND CUSTOMS ENFORCEMENT, DEPARTMENT OF HOMELAND SECURITY, WASHINGTON, DC

Mr. EVERITT. Good morning, Chairman Grassley and Senator Bingaman. I am pleased to be here today to discuss the technical aspects of fraudulent documents.

The U.S. Immigration and Customs Enforcement Forensic Document Laboratory, known as the FDL, is the premier forensic document laboratory in the world and is dedicated exclusively to the detection and deterrence of fraudulent documents.

The FDL is accredited by the American Society of Crime Lab Directors' Laboratory Accreditation Board on questioned documents and latent prints. The FDL's mission is to detect and deter domestic and international travel and identity document fraud by providing a wide variety of forensic and support services to all DHS components, and other Federal, State, and local agencies, as well as foreign government, law enforcement, and border control entities.

There are misconceptions about what constitutes a fraudulent document. Many people think that fraudulent documents are simply counterfeit documents. While counterfeit documents are, in fact, fraudulent documents, the term "fraudulent documents" also includes altered and fraudulently obtained documents.

Altered documents are genuine documents with erasures, substituted photos, and thin-layer laminate overlays. Fraudulently obtained documents are genuine documents that have been obtained by fraudulent means.

Whether counterfeit, altered, or fraudulently obtained, their purpose is to allow the bearer privileges or benefits to which they are not entitled.

Stolen blank documents also pose a serious threat. Over the years, the FDL has seen many stolen blank passports which have been personalized to create fraudulent documents. These documents are particularly hard to detect.

The FDL sees many types of fraudulent documents originating from locations all over the world. We also see fraudulent documents of various quality. These include documents that are obviously fraudulent upon inspection, and range up to high-quality documents that can only be confirmed using sophisticated equipment for forensic examination.

In addition to the services we provide to field units, the FDL also directly supports ICE investigations targeted against the producers and distributors of fraudulent documents. We also support the ICE Document and Benefit Fraud Task Forces which were established in April of this year in 11 cities across the United States. These task forces have already achieved significant successes, and ICE is evaluating the expansion of these task forces to additional locations.

Fraudulent travel and identity documents are a worldwide problem which will continue to challenge law enforcement officials in the United States and abroad. As long as identification is required to travel and obtain goods, services, or jobs, criminals will attempt to produce fraudulent documents.

ICE has had many successes in stopping several major fraudulent document production and distribution operations, including the Castorena Family Organization and the Mandalapa Organization.

These investigations resulted in numerous indictments and arrests, the seizure of millions of dollars in illegal proceeds, and tens of thousands of fraudulent documents. ICE special agents across the country continue these same type of investigations today.

In order to deter and detect fraudulent documents effectively in the field, the FDL believes there needs to be a triad approach. This triad approach includes: (1) strong documents using the latest materials and technologies for the production and incorporation of the latest security features; (2) electronic systems to validate the existence of the document and the information contained within; and (3) a biometric link that will tie the person presenting the document to the document and to the electronic validation.

In order to work properly, each of these three elements of this triad system must be as strong as possible, including the documents. This is not only to ensure the integrity of the triad system, but also to allow the documents to stand on their own in the event that the technology systems are not available.

The development and distribution of this system will be expensive. It will require replacing current document production systems and infrastructure and the integration of new technologies. However, we believe the investment in this system would pay healthy benefits and dividends in increased security and faith in our identification system.

On behalf of the men and women of ICE, and specifically the men and women of the Forensic Document Laboratory, I thank the Finance Committee and its distinguished members for your continued support of our work.

I would be pleased to answer any questions you might have at this time.

[The prepared statement of Mr. Everitt appears in the appendix.]

The CHAIRMAN. Yes. If it is all right with Senator Bingaman, I think we will take 10-minute round turns. Is that all right, as long as there are only two of us here?

Senator BINGAMAN. Sure.

The CHAIRMAN. All right.

To Mr. Kutz, your investigators have been getting through checkpoints with fake IDs for nearly 4 years. In total, according to the chart that we have, 93 percent of the crossings were unhindered. They do not seem to be getting much better at it during that period of time.

Did the Government Accountability Office investigators see any improvement since our 2003 hearing that made it harder for them to cross the border with fake IDs?

Mr. KUTZ. No, not really. I think that the current system, as I mentioned in my opening statement, is vulnerable to people entering the United States from Canada and Mexico, or other locations, using counterfeit documents.

So I am not sure it is reasonable to expect the human element of people at the border, with the current technology they have, to be able to identify counterfeit driver's licenses and birth certificates. There are too many variations and too many other types of variables involved. From a security standpoint, more of a standardized process is going to be necessary to secure the border.

The CHAIRMAN. All right.

Mr. Ahern, I have three or four questions. They are all kind of hooked together, and they are not complicated.

Just, an explanation of why your agency has not gotten any better at catching these phony IDs since our last hearing, how long it might take, and how many hearings we would have to have to bring this to the attention of the agency to maybe handle the problem, and just, if we were, for instance, to have such tests a year from now, would you predict that your agency's failure rate would be better? Is there a certain number of years that you might predict? I am just saying 1 or 2 years.

Mr. AHERN. Well, Senator, what I would offer as an answer to that, first off, when we take a look at documents that are admissibility documents, driver's licenses and birth certificates are not acceptable documents for admissibility.

We train and have our officers focus on those documents that are legitimate admissibility documents that are government issued, that are adjudicated, that actually verify identity, and also their nationality and citizenship. Those are passports, border crossing cards, permanent resident cards, and laser visas.

As I said, we have 84,000 of those that we actually intercepted in the last year, so that is our focus. Those are the individuals who pose a risk to this country, who are coming in with those types of false documents, not American-born U.S. citizens who work for the Government Accountability Office with a driver's license coming into this country.

But your question is, what are we doing to move forward? We are looking at bringing on additional equipment, and also for training for officers on the driver's licenses.

As you have pointed out, that is a vulnerability. Until we actually have the WHTI with standardized documents, 18 months from now, in January of 2008, we will have that vulnerability where people could exploit that.

I want to provide some level of confidence to you, sir, that we are very adept at identifying those documents that truly could be used against us for risk by people of foreign-born nationality who are coming into this country. Those are passports, border crossing cards, and permanent residency cards, that we do intercept with great regularity.

The CHAIRMAN. Mr. Everitt, I am wondering about the typical quality of fake documents that you see at your Forensic Laboratory. Approximately how many are sophisticated enough that a CBP inspector could not tell that they are phony simply by looking at them?

Your office conducts extensive training of other agencies such as CBP on how to recognize fake documents. Officers at primary inspection points only have a little time to look at documents and decide whether they are phony. There are over 240 valid types of driver's licenses and hundreds of other kinds of identity and travel documents.

The second question is, how can we possibly train a front-line inspector to memorize all the security features in all of these documents well enough to catch the fakes by looking at them in only a few seconds?

Mr. EVERITT. Senator, if I may answer your second question first. We cannot train people to recognize the individual security features in all those different documents. It is too much information.

What we do is, we train on security features that are incorporated in documents, and to look for those security features. Many security features run across a wide variety of documents. What we believe is that we need to create better-quality documents across the board.

If I can show this, I would like to put up a display of a Virginia driver's license. There are two examples of a Virginia driver's license. As you can see, they are very, very close.

What you are actually looking at is, the driver's license that is on your left is counterfeit, the one that is on the right is authentic. It would be hard for most people in the field to recognize that counterfeit driver's license. It is very, very close to the original. Actually, without having the authentic driver's license up there with it, it would be almost impossible to tell the two apart.

The first part of your question, as I answered before, we do provide the training on the security features in the documents and we provide that not only to CBP, but to agencies throughout the government, and also around the world. It is a difficult task because we have so many different documents.

Unfortunately, our documents tend to lag behind in technology, to where the technology that is used to create the documents becomes commercially available and is widely available to anyone who has the money to purchase it, and it has actually come down in expense over the years.

What we need to be doing is, we need to be pushing forward very diligently to bring in the new technologies to make stronger documents as those technologies come on board.

The CHAIRMAN. Mr. Kutz, how easy was it to create fake documents that were used by your agency to cross the border?

Mr. KUTZ. We do it all the time, actually. We do it, between Mr. Cooney's and my office. We use, again, as was mentioned by Mr. Everitt, publicly available hardware, software, paper stock, or plastic, whatever you are talking about. So I would say, to make a counterfeit driver's license is not very difficult. To make a very good one would be much more difficult.

I would add, with respect to things like passports, I believe passports would be much, much more difficult. We have not counterfeited passports before, but I believe they would be much more difficult to do. So I think, from a security standpoint, again, documents like that would be much more difficult to counterfeit.

The CHAIRMAN. Mr. Everitt, we have asked to see the tools that the Department of Homeland Security provides officers at primary inspection points to catch documents like fake driver's licenses.

We got this booklet that is called "ID Checking Guide," and it would have different documents, driver's licenses for the various States. This is what we got. I understand that you brought to the hearing some other tools that you have. Could you tell us what those are?

Mr. EVERITT. Yes, sir. When we provide the training, one of the things that we provide is called a 10× loupe. It is simply a magnification device that you look at a document with to magnify the security features that are on there to identify the security features. It is effective. There are security features that cannot necessarily be seen with the naked eye, but can be seen with a magnification device of this type.

We also provide a black light and a flashlight. The black light allows you to see ultraviolet security features. The flashlight can be used as a combination device. The flashlight can be used not only to put more intense light on it, but also to use it at angles to show features that show up with side lighting.

The CHAIRMAN. Is there any other technology available in a primary inspection booth to detect fake driver's licenses?

Mr. EVERITT. Sir, I would have to pass that question to Mr. Ahern.

The CHAIRMAN. All right.

Mr. Ahern?

Mr. AHERN. Senator, no, there is not.

The CHAIRMAN. All right.

Mr. AHERN. Just to give a broader answer on that as well. Until we have a standardized document that has biometric security features inside, and also has machine-readable capabilities so our primary officers can run it against our border integrated systems for watch-listing and for NCIC fugitives, we will have this same type of a hearing periodically, sir, until we actually have the full security capabilities on the primary borders of this country.

The CHAIRMAN. All right. So until the perfect document comes along then, there is not anything you are going to try to do between now and then.

Mr. AHERN. That is not my response, sir. To be able to provide the level of security that you and this country expects, we need those standardized documents with machine-readable capabilities that have security features imbedded in those documents.

What we are continuing to do, though, is to provide the training. We have taken several steps since the GAO investigations to provide that book that you just showed to the panel here, as well as training musters and awareness toward individuals.

In fact, yesterday I was in Detroit, seeing what a private sector solution might be for us to look at verifying documents. The particular piece of technology I saw was a reader of a driver's license that was taped to the top of a laptop. That is not an acceptable piece of technology for our border officers. All it did was go against 9 States' databases to find out whether it is a legitimate document or not.

So we need to have something that not only gets all 50 States for all versions that are out there in those 50 States, which can be over 170 or 180 versions, I am told, and also something that goes against the watch list of this country and our fugitive database, and our look-out systems that we have at air and seaports today.

The CHAIRMAN. All right.

Senator Bingaman?

Senator BINGAMAN. Thank you, Mr. Chairman. Thank you all for being here.

Let me just try to understand, the best I can, what is involved. When we are checking people coming in at our borders, the ideal would be to have everybody with a passport, I guess. I mean, my impression is, Mr. Kutz, I think you said that it is more difficult to make false passports, or that is your impression.

Mr. KUTZ. Yes. I would agree with what Mr. Ahern said, too. The biometric really is what is the most secure. But certainly of what is out there now, the passport is much better than a driver's license or birth certificate.

Senator BINGAMAN. And the job of the inspector at the port of entry is to say, this person is the person who properly owns this passport, who was properly issued this passport.

Second, this person is not on one of our watch lists and we have no objection to this person entering our country. That is the machine-readable part, I guess, or to basically calculate a check-back with some database and make sure that, whoever it is who has this passport, once we have determined that it is a valid passport, is not somebody we want to keep out of the country. Am I understanding that right so far, Mr. Ahern?

Mr. AHERN. Thank you. That is essentially correct. If I might just walk through those, I would appreciate that.

Senator BINGAMAN. Yes. Go ahead.

Mr. AHERN. First off, in the air environment, it is the best example we have. Your question is, would we prefer a passport for land border solutions? Certainly that would be the gold standard.

But as we are looking forward to the implementation of WHTI in January of 2008, we need to take a look at what is something that is an equivalent document. Secretaries Rice and Chertoff have looked at what might be an equivalent to a passport with some security features.

It might be a wallet-sized card referred to as a PASS card that would have some of the same security features, and also the same machine readability. That, we are still exploring between our two departments.

But, clearly, what we need to have is a document that has been adjudicated by an official of a government that we have confidence in, something that identifies the citizenship of that individual and that we can verify through security features in that document and biometrically match that person, much like we do at airports today with the U.S. VISIT program.

We have an individual who comes in, and we do finger scans on primary to match that person against the document that they received overseas and the visa they were issued overseas, to be able to match that person. That is a huge security feature that we have. We need to have those types of things replicated in all environments.

Senator BINGAMAN. Let me try to understand. There seemed to me to be various initiatives moving forward here to meet these needs, and I am not sure how they integrate or relate to each other. There is this WHTI card that you have referred to, I believe.

Mr. AHERN. WHTI is not a card. WHTI is an element of the Intelligence Reform and Terrorism Protection Act which calls for standardized documents for January of 2007 for air and sea, and January 1, 2008 for the land environment.

Senator BINGAMAN. All right.

There is also this PASS card that you just referred to. I guess, the Secretary of State would be issuing PASS cards, at the urging of Homeland Security. Is that right?

Mr. AHERN. We are working collaboratively with the Department of State and with the Department of Homeland Security, and with the Government of Canada, also, as far as what might be an acceptable standard of documents.

We are looking at, certainly, the passport being the gold standard solution, but realizing that the adjudication and issuance of passports for people that do a lot of multiple cross-border travel may not be realistically feasible.

But we would not settle for anything less than something that is as secure and has biometrics, as well as something that has machine readable capability.

Senator BINGAMAN. So what you are driving toward, getting to, is where everybody coming through a port of entry would have either a valid passport or a PASS card. Is that an accurate statement or not?

Mr. AHERN. What I would say, sir, is that is very accurate. I began my career as a front-line officer 30 years ago on the border with the U.S. and Mexico in San Ysidro, CA.

As I look 30 years later, we need to provide a level of security to identify individuals coming into this country, to run it against the watch list, determine their citizenship, and we need to make sure that we have a standardized document that has the biometric features, whether it is a passport or a PASS card, that is machine readable.

Senator BINGAMAN. But it has to be one of those two?

Mr. AHERN. Something that meets that standard, certainly. We are taking a look at if there are other types of documents that meet those standards, but that is what we are looking at as we move forward.

Senator BINGAMAN. All right.

Now, we also legislated here in the Congress a requirement called the Real ID requirement to be implemented by May 11 of 2008. That calls for standards being imposed upon the issuance of driver's licenses by the various States, as I understand it. How does that requirement by the Federal Government relate to these other various things that you are talking about here?

I mean, if we are not going to allow people to use these driver's licenses to get into the country at any rate, then it is not relevant to that screening process, I guess. It would be relevant to other screening process. Is that accurate?

Mr. AHERN. Well, I am more familiar with the WHTI requirement for admissibility. A driver's license does not adjudicate citizenship. It does not indicate their citizenship. The Real ID would provide a secure document that gives the individual permission to drive.

Oftentimes, a driver's license is one form of identification that can be used for the application of a passport, so any security you could add into that certainly would be important. But as I take a look at, again, border requirements, what we need are standardized documents that are provided for under WHTI.

And another point as well. There are other programs that we want to take a look at tying in. Currently, as you are aware, being from New Mexico, we have our cross-border travel program, the SENTRI program, a fast program for truck drivers where we vet them, adjudicate them, and provide them a secure document to do expeditious crossing across the border.

We have 225,000 people enrolled in those programs on the northern and southern border. Those features will be rolled into a WHTI requirement because we want to continue to sort out those at a very low risk and expedite their crossing so we can focus on individual concerns. But it focuses back on a standardized document that we can read.

Senator BINGAMAN. This Western Hemisphere Travel Initiative. What is the time frame for getting this done? When will it be to a point where we can legitimately say everybody coming through our borders has been inspected to determine whether they have a valid passport, or a PASS card, or whether they are on some other list of preferred entry that we have set up?

Mr. AHERN. Well, we did an Advanced Notice of Proposed Rulemaking last year. We received over 2,000 comments. Oddly enough, most of them were from Canada. Most of the people were interested with the cross-border travel with Canada and the United States.

We currently have our Notice of Proposed Rulemaking at OMB for review for the January, 2007 implementation of the air and sea aspect of the Western Hemisphere Travel Initiative, and we are in the developmental stages of the rulemaking process for the land solution that is due for January of 2008.

Senator BINGAMAN. So in January of 2008, you would expect at that time to have in place a system for requiring this kind of identification by everybody coming across in our land-based ports of entry? Is that what I understand?

Mr. AHERN. That is what the current target is, sir. But as you know, there are different bills being introduced to delay that implementation.

Senator BINGAMAN. The push-back to delay the implementation is primarily because of what?

Mr. AHERN. Well, I cannot speak to why individuals might have introduced the legislation or bills, but I can certainly recall, from looking at some of the 2,000 comments that people made to the first Notice of Proposed Rulemaking or the Advanced Notice of Proposed Rulemaking last year, a lot of people just feel it is not necessary. A lot of different industries think it will hurt their industry. A lot of the communities on both borders think that it will impact cross-border trade.

Some think it will impact cross-border travel, and it would impact communities on both sides of the border. I believe that, through a well thought out solution and a very efficient process of issuing of documents, and even looking at alternatives to the standards—not alternatives to the passport, but something that meets the standard—can certainly accomplish what the goals are for security, and also the efficient cross-border movement of people.

Senator BINGAMAN. Now, what is the timing for issuance of these PASS cards? If I wanted to get one of these PASS cards, when would I be able to apply for it, and what would be the process?

Mr. AHERN. Those dates have not been set. We are still in the formulation stage of that. That will be part of the proposed regulation that would be developed and issued for the land solution, which has not gone out. Only the air and sea environment has actually made its way through the department into OMB at this point in time.

Senator BINGAMAN. So the air and sea environment contemplates that everybody coming into the country by air or by sea have a passport?

Mr. AHERN. It would be inappropriate for me to tell what the actual final rule is until it clears and actually gets issued, sir.

Senator BINGAMAN. So it is possible that we would allow some other forms of identification to also serve to allow the entry of people coming here by air or by sea.

Mr. AHERN. I would say, again, the passport is the gold standard. We would need to make sure that anything less than that has the same security features, is machine readable, and is something that is an acceptable alternative.

Senator BINGAMAN. Other than the passport and the PASS card, what meets that criteria?

Mr. AHERN. There would be some documents that we could talk about, but I would really prefer, sir, until we actually clearly go through the rulemaking process, I would not want to be contrary to the Administrative Procedures Act.

Senator BINGAMAN. All right. Thank you, Mr. Chairman.

The CHAIRMAN. I had several other questions. I am just going to ask a couple, then probably submit the rest in writing. Then for this panel, as well as the other panel, there are members who could not come because of conflicts, so maybe you will get questions for answer in writing.

We would ask the staff to tell their members to get those submitted by 5 this afternoon; I may be more lenient depending on what my staff says is more appropriate. Then if you could get answers back as soon as you can, we would appreciate it.

I would ask, Mr. Kutz, this is following on where I left off with Mr. Ahern. During any of the times that you were trying to cross the border, did CBP ever swipe or scan the driver's license that you used through any of the electronic readers?

Was there a time when you thought that they might scan your license, and if so, would that make you a little nervous about getting caught coming into the country?

Mr. KUTZ. In answer to that, I am going to give Mr. Cooney a chance to answer that, since he is one of our agents who actually made the crossings, if that is all right.

The CHAIRMAN. All right. Mr. Cooney?

Mr. COONEY. Yes, Senator. At one port of entry on the southern border, the license was not scanned. We thought it was. We took precautions to enter the country and have a story if the license was scanned.

When we got to the port of entry, we found ourselves in an empty room with three CBP officers and we had to do a little quick talking, socially engineering the situation, after which we were never asked to show any identification. We were just asked if we were U.S. citizens, and then told to come into the country.

The CHAIRMAN. All right.

Mr. Everitt, according to Mr. Ahern's testimony, CBP has spent money establishing a Fraudulent Document Analysis Unit. That sounds a lot like the title of your office, Forensic Document Laboratory.

Mr. Ahern's testimony also says that one of the things that CBP did was to deliver "state-of-the-art fraudulent document work stations." I believe he is referring to some very expensive machines designed for a laboratory environment, not something that could be deployed at a primary inspection point. So, it looks like they are duplicating your efforts rather than using their resources to give front-line officers the tools they need to do the job of primary inspection.

Would you explain the difference between the tools that might work in secondary inspection and in a lab, and the kind of tools that are needed for primary inspection?

Second, and last, how much do each of these laboratory-style work stations cost?

Mr. EVERITT. Senator, I believe the tools that you might be referring to are ones that we have in the laboratory called Video Spectrum Comparators. We have several models within the laboratory. They range in price anywhere from $30,000 per unit to $90,000 per unit. They are very expensive.

They are used by the forensic document examiners in the forensic examination of a document. They are quite technical. I would not believe that they would be appropriate for a primary lane, only because of the size. They are large. They would require quite a bit of training to operate and are probably not appropriate for a primary application.

There are some technologies that are available on the market that we have not looked at, as it is not the job of the Forensic Document Laboratory to evaluate those machines that may be suitable for primary application. They basically give a red light/green light on a document as to whether it is authentic or not, based on comparison with a known document that is stored in the database. Those may be appropriate for primary application. Like I said, though, it is not something that we would evaluate.

The CHAIRMAN. All right. I will not ask any other questions. But maybe I should give any of you who want it an opportunity to say one last thing before we bring in the second panel. I would be glad to give you a little bit of time.

Mr. Ahern?

Mr. AHERN. Sir, if I could just add on to Mr. Everitt's comment, certainly the technology we deployed for document detection is a secondary technology. It is not for primary.

For primary, secure documents are needed that can be machine-read. We have done a lot of issuance of machine readers. Most every one of our 805 primaries we have on both borders are equipped with machine readers, document readers.

What we need to get is documents that can be read beyond just the current number of passports—border crossing cards, permanent resident cards, and laser visas—that can actually be swept on primaries and run against our systems to be able to make good determinations of who is coming into this country.

The CHAIRMAN. All right.

Anybody else?

Mr. KUTZ. I would say one thing. When we deal with Customs folks, I just want to say that we have a very positive relationship. When they hear from us, it is not usually good news. So I want to just say that usually they act in a very proactive and constructive manner in working with us, and I do appreciate that, because a lot of people are not very happy to hear from us usually, Senator.

The CHAIRMAN. All right. Thank you all very much.

I will call the second panel now. I have not introduced the second panel, so I will do that. Come while I am introducing you.

This is to learn what the private sector is doing to protect itself, what State government is doing to validate IDs, and what other countries are giving border inspectors as tools to catch fake documents.

Our first person is Janice Kephart, former counsel of the 9/11 Commission and an expert on terrorist travel; second is David Shepherd, who is director of security for the Venetian Resort Hotel, an establishment that protects more than 50,000 visitors and millions of dollars a day. He will testify about how they use scanners to verify documents. A third witness is Mr. Bruce Reeves, CEO of AssureTec Systems, which has developed an advanced technology, in use in countries like Chile and Singapore, to check for fake documents; and then, last, Scott Carr is executive vice president of Digimarc. He will be testifying and demonstrating how such technology could better work together to help protect our borders using security features already in millions of driver's licenses.

I thank you all. We will go in the order that you were introduced. So, you start out, Ms. Kephart.

STATEMENT OF JANICE KEPHART, PRINCIPAL, 9/11 SECURITY SOLUTIONS, ALEXANDRIA, VA; FORMERLY COUNSEL TO THE 9/11 COMMISSION

Ms. KEPHART. Thank you, Chairman Grassley, for having me here today to talk about how and why we need to ramp up our U.S. border inspection policies and practices.

I do not think I need to remind the committee that it has been nearly 5 years since 9/11, and border inspection has shown little improvement. The slate of 9/11 hijackers, you might recall, had a 97-percent success rate at entering the U.S. by passing inspectors 34 of 35 times.

Today, GAO tells us that in 45 attempts at entry over our land borders with fake documents between 2002 and 2006, they were successful 42 times, or a 93-percent success rate.

In 2006, GAO had a 100-percent success rate at illegal entry. In this 2006 study, perhaps the most troubling finding is that, when CBP officers in Michigan and New York did their jobs the best they could and asked for identity documents and tried to compare them to verify identities, they were stifled by a complete lack of any tools to help them authenticate as fake or valid the documents presented to them.

Without being able to make a determination that the documents were fake and the agents inadmissible, the government agents were allowed in, as is standard immigration policy.

Now let me step back and retrace our steps as to why the 9/11 Commission unanimously recommended that we need to ramp up our border inspection process, require a passport or equivalent at our ports of entry, and the threat the Commission's border recommendations seek to mitigate.

We need to ramp up our border security and stop encouraging the use of fake documents, because we know that terrorists are trained in document forgery and travel techniques.

Reviewing GAO's study, it is not difficult to be concerned that GAO's success rate at illegal entry could be easily translated into a potential success rate for terrorist entry. In fact, while I cannot state specifics in an open hearing, I can tell you that, during my tenure on the 9/11 Commission, we were privy to information—information not even included in our staff monograph—that gave us good reason to be concerned that varieties of fake documents have been a modus operandi for terrorist entry into the U.S. for years now.

We also know that terrorist travel poses a specific threat, because terrorists usually require travel across borders to conduct operations. To do so, they will exploit any loophole in a border apparatus that they can. An extremely large loophole that still exists today here in the U.S., are the policies and practices that permit anyone claiming to be from the Western Hemisphere to present easily forged documents, or nothing at all, to enter the U.S.

The most commonly used documents include a birth certificate, tens of thousands of varieties, a driver's license, over 240 varieties in the U.S., or, as is the case with 40 percent of Canadians that pass over our land borders according to Zogby surveys, absolutely nothing.

We know birth certificates and driver's licenses are highly subject to fraud both in the U.S. and throughout the Western Hemisphere. DC sniper John Allen Muhammad and LAX Millennium bomber Ahmed Rassam both made their living on stealing, making, and selling fake U.S. or Canadian documents prior to coming to the U.S. for their criminal acts.

The 9/11 Commission recommended the use of passports or a biometric equivalent because, while no travel document is perfect, passports have features other documents do not: they denote citizenship; they can be vetted through criminal and terror watch lists and alerts; national records are maintained on the passport owner, so reported lost and stolen passports can be better tracked internationally. They have particular security features, usually more difficult to forge.

From the terrorists' vantage point, they know we cannot verify identities with a driver's license today at our ports of entry, nor authenticate a license as legitimate, so why not take advantage of U.S. laxity and use a fake?

To briefly review the threat, recall that Canada's intelligence service tells us that they are watching at least 350 terrorists, yet Canadian law enforcement is so curtailed by Canada's post-9/11 anti-terror laws, that there has been only one indictment, up until the bust of the 17 in Toronto in June.

In addition, the FBI has million-dollar bounties on a number of Canadian-based al Qaeda members who have directly threatened the United States. Recall, too, that south of the border, Mexico is known for al Qaeda seeking entry through there, both at land ports and over the physical borders; Hezbollah has smuggled in 200-plus of its sympathizers; and the Caribbean is a hot-bed of terrorist activity.

Let me be clear, though, that assuring facilitation of trade and tourism is also important. To do so, we need to give border inspectors the technology, training, information, and policy support together to focus on high-risk travelers, while low-risk travelers can get streamlined and efficient processing if they seek to do so, thus securing facilitation equally and providing the necessary policy of objective balance. With support from the private sector, I believe that that balance is highly doable.

So where does the terrorist end up with border inspection as it should be? With a difficult choice. With better-trained inspectors with access to better information and better technologies, and expertise in a few acceptable forms of travel documents instead of thousands, the terrorist can no longer expect to get away very easily with presenting an unauthenticated document containing unverified information.

Instead, the terrorist must choose now: risk getting caught by attempting an illegal entry, or risk being detected by U.S. authorities at the border when presenting a passport or equivalent.

Ramped up border security makes it more likely that the terrorist will expose himself to authorities, giving the American people a better chance at keeping a garden variety of dangerous foreign terrorists out of the United States.

Thank you.

The CHAIRMAN. Thank you, Ms. Kephart.

[The prepared statement of Ms. Kephart appears in the appendix.]

The CHAIRMAN. Mr. Shepherd?

STATEMENT OF DAVID SHEPHERD, DIRECTOR OF SECURITY, VENETIAN RESORT HOTEL, LAS VEGAS, NV; FORMERLY WITH THE FEDERAL BUREAU OF INVESTIGATION

Mr. SHEPHERD. Thank you, sir. Chairman Grassley, distinguished members of the U.S. Senate Committee on Finance, ladies and gentlemen, thank you for the opportunity to testify before this very important committee concerning border security.

Currently, I am the co-chairman of the Gaming Resorts Subcouncil for the Commercial Facilities Sector Coordinating Council; a member of the Partnership for Critical Infrastructure Security; a member of the Real Estate Round Table Terrorism Task Force; and a member of the Las Vegas Security Chiefs Association. In each of these capacities I represent only a small portion of the private sector, and I am honored to be a participant.

In the private sector, the identification of customers, employees, and business partners is important in protecting the property from criminals, terrorists, and from individuals who attempt to bypass existing laws and regulations.

Because of the possibility of misidentification of those who could do harm to individuals or to a business, financial reporting requirements—the Securities Exchange and Commission, Office of Foreign Asset Control, Sarbanes-Oxley, and gaming control regulations—were enacted by those agencies with foresight on the identification of individuals.

Each private sector business has an obligation to its employees, guests, and the community at large to know the identity of individuals who interact with the company. The private sector partners are cornerstones of the entire community; thus, safety is the underlying common element for proper identification recognition, not the potential for fines or business restriction if non-compliance is uncovered by a regulatory agency.

Regardless of the fake driver's licenses used by a seemingly innocent under-aged individual attempting to gamble in a casino or enter a nightclub, that same fake driver's license in the hands of a criminal could have significant financial impact on property through fraudulent financial transactions, in the form of existing or extending credit, application for a loan, or credit card purchases. In the hands of a terrorist, the catastrophic events of 9/11 or the London train bombings could be repeated within our borders.

The fake identification is a means to an end, and the choice of that end is the possessor's. Las Vegas has already seen the face of terrorism, as eight of the deadly hijackers visited my city prior to 9/11. Unfortunately, those were never detected by the individual systems in place.

If you will look at the monitor, we will present different fake and real identifications. Speed and accuracy in recognizing false identifications are important elements in a system of protection for a business.

Determining if a person is 21 before he or she is served alcoholic beverages, or if the individual is actually John Doe before extending a line of credit, or even offering a position within the company to a seemingly qualified applicant cannot be left to chance or to an individual's discretion.

Unfortunately, there are over 10 million cases of identity theft in the United States each year. The Internet provides instructions on how to create false identification.

Technologies have been used by the criminal element to replicate fake identifications, regardless of the State or country of origin. Thus, technology should be employed to keep ahead of those who attempt to circumvent the system.

I have had an opportunity to review various technologies and systems currently available within the private sector which offer full or partial solutions to security and regulatory challenges under financial, criminal, civil, risk management, and terrorism concerns.

In the commercial facility sector, many private partners have deployed systems to identify fake driver's licenses, passports, and visas offered as proof of identification. One of the systems that is here is available today.

In addition to this system, there are other systems available that currently focus on driver's licenses or credit cards, without referring to reference manuals and without unduly inconveniencing those individuals who are being screened.

Thank you for the opportunity to speak.

The CHAIRMAN. Thank you, Mr. Shepherd.

[The prepared statement of Mr. Shepherd appears in the appendix.]

The CHAIRMAN. Mr. Reeves?

STATEMENT OF BRUCE REEVES, CEO, ASSURETEC SYSTEMS, MANCHESTER, NH

Mr. REEVES. Thank you, Chairman Grassley and other members of the committee. First, we also want to thank you for inviting us to give testimony regarding commercially available technologies to assist our border inspectors in detecting fraudulent documents.

AssureTec Systems of Manchester, NH is one of the companies providing automated document authentication technology. It has already been established, and we certainly want to weigh in and agree, that the issue we are dealing with here is not the fault of the border agents who are serving our country in a very valiant way.

The problem, really, is the issue that technology needs to be made available, real-time, with both accuracy and significance, that in effect can log in a transaction so we know who, in fact, has crossed the border, as well as determining the validity, or at least the risk factor, of the documents presented.

I have been specifically asked to address three basic questions: first, the current viability and availability of the technology; second, examples of the technology in various places and by other governments; and finally, an estimated cost for adding this technology to a typical U.S. border.

Our company delivered its first technology border product in February, 2004. I have on the board—I will not speak specifically to it because there is not time, but would be open to questions—a schematic for a system of automated document authentication which, in effect, becomes an exit/entry system in the country of Chile.

This technology has been integrated by the Chilean government to include document exit/entry and picking up of the information that is being delivered when someone crosses a border. An attempt has also been made to take state-of-the-art biometrics and move those into the solution with existing documents.

This solution operates behind the scenes and, in a few seconds, delivers an alert, very similar to what you have seen, in this case on the border, in the event the system detects a problem or exceeds a particular level of risk.

When alerts are encountered, the operator or the border agent can click on the specific item for further detail and drill down.

A similar border management solution has recently been installed by Merit Technologies of Melbourne, Australia in Papua New Guinea for a totally integrated border exit/entry system. There, they also included the capability to match, in addition to watch lists integrated with our technology, solutions to vet passenger manifest systems that are sent to the U.S. and other countries involving flights in and out of the country.

Our systems are currently being used daily in both Thailand and Singapore in the e-passport enrollment process for the issuance of new electronic passports that will be used around the world. In short, the answer to the question is that the technology is readily available off the shelf, and is being deployed by other governments.

Our system is installed in a particular U.S. embassy in an area where documents are very suspect, and in the course of review of about 25,000 documents that are used to get visas to enter the United States, hundreds of bad documents and fakes have been found.

For the past 18 months, our system has been deployed in the Transportation Worker Identity Credential, TWIC, program, Phase III, which now is in the process of being reviewed for deployment to the next level. That has been used for approximately 18 months.

The third question was trying to estimate the price. Our company does not typically provide end-user application pricing. We normally work through systems integrators around the world.

In this case, using the GAO's recent analysis that on the order of 300,000 to 400,000 entries are made at the U.S. borders, and estimating about 80 to 85 percent are land borders, I would say that, with the 500 or so lanes that are currently being utilized by border inspectors in the land borders, that the cost of our typical technology of the high-end product would be in the range of about $4,000 to an integrator, perhaps twice that number on a solution and integrated basis, and would operate approximately at a cost of between a third of a cent per crossing to less than a penny per crossing on an integrated basis, using a 3-year model.

To conclude, we believe automated document authentication is both commercially available and economical. Thank you for inviting me to testify today, and I am willing to answer further questions if you wish.

The CHAIRMAN. Thank you.

[The prepared statement of Mr. Reeves appears in the appendix.]

The CHAIRMAN. Now, Mr. Carr?

STATEMENT OF SCOTT CARR, EXECUTIVE VICE PRESIDENT, DIGIMARC, BEAVERTON, OR

Mr. CARR. Chairman Grassley, thank you for the opportunity to appear today before the committee to testify.

I come to you from Digimarc Corporation. We are the leading provider of citizen identity documents in North America. We produce 60 million secure IDs a year, including two-thirds of U.S. driver's licenses.

We are also an innovator in a technology known as digital watermarking. This technology has been used in currency, identity documents, music and movies, to deter piracy and counterfeiting.

In fact, in 2002, States began to adopt this in driver's licenses as a machine-readable security feature to authenticate those documents. Eighteen States have adopted digital watermarking as of today, including States like Florida, Texas, Massachusetts, Iowa, Nebraska, New Jersey, and Michigan.

In Michigan, more than 75 percent of the circulating licenses contain digital watermarks. This feature can be authenticated at the border in seconds to detect fake IDs.

We, too, were asked to estimate the cost of deploying the technology, and while we do not have all of the information about the extent of the deployment, our estimate is that readily available technology that has been proven and is available could be deployed in 6 to 12 months, at a cost of less than $50 million.

Digital watermarking is compatible with the Western Hemisphere Travel Initiative, with Real ID, and with the U.S. VISIT program. It is used to secure driver's licenses and could also be used to secure passports, the proposed PASS card, Federal worker credentials, and other forms of travel documents.

We commend the committee's efforts to challenge all of us to improve U.S. border security, and we recommend that machine-readable authentication of driver's licenses and other identity documents be conducted at the U.S. borders, and that this include machine-readable authentication of the digital watermark.

We support closing the Western Hemisphere travel loophole, and in fact believe this can be accomplished by harmonizing WHTI and the Real ID program.

What I would like to do now is demonstrate how some of this technology works. What we have are two Nebraska driver's licenses which, if you look at them, appear identical. In fact, the name and demographic data on the front of the cards are the same. What is different are the photos. The pictures of the people are different. One of these IDs is fake.

Simple visual inspection is not going to determine which is which. My colleague will place the document in a readily available scanner. This scanner will scan both sides of the document, essentially taking a picture of the front and the back.

The software will decode the bar code, read the digital watermark, and inspect other features that are found in the document to determine if, in fact, it is authentic. You can see here by the green indicator that this is the valid ID.

This technology has been deployed in the States, and in fact a pilot was funded by the U.S. Department of Transportation in Nebraska, where readers were deployed in police cruisers, convenience stores, bars, nightclubs, and other public events. One hundred percent of the users found that the use of digital watermark-based authentication gave them confidence that the document was, in fact, authentic.

We will take the second ID now and repeat the process. Again, we place it in this readily available scanner, we scan the document, and as you can see, we detect that, here, the photo has been swapped. This is the fake ID. Digital watermarking allows you to detect photo swapping, data alteration, and other forms of common counterfeiting.

As I mentioned, digital watermarking is compatible with WHTI, U.S. VISIT, and other forms of travel documents. Here, we will switch to a different reader where we will scan the document as we did before, we will read the 2–D bar code, and we will allow the scanner to read the front of the document.

In this case, it is a Massachusetts driver's license. Here, we will do complex pattern recognition, we will read the digital watermark, and we will compare all of that information to determine that this is, in fact, a valid ID. This authentication can happen in seconds.

The technologies are readily available today. The equipment that you see on the table in front of you is sufficient to equip three lanes at a border crossing. We believe that these can be deployed to enhance the security of the U.S. border.

Thank you for the opportunity to testify.

[The prepared statement of Mr. Carr appears in the appendix.]

The CHAIRMAN. I am going to start with you, Mr. Carr, and Mr. Shepherd. Do you believe that if these scanners had been installed in all of our primary inspection points, that the Government Accountability Office would have been caught when they showed their fake driver's license?

Mr. CARR. Mr. Chairman, we do believe that we could have caught the fake IDs that the GAO used to cross the border.

The CHAIRMAN. Mr. Shepherd?

Mr. SHEPHERD. I believe the same thing, sir.

The CHAIRMAN. All right.

Now, of course, the witnesses from the Government Accountability Office are still here and they have the fake driver's licenses with them that were actually used to cross the border. I would like to have your personnel run them through the scanners and see what happens.

Now, for security reasons, I would like to ask the press not to take any photos of the television screen during this demonstration.

Mr. CARR. As you can see, my colleague is scanning the document in the same way we did in the prior test. The software is analyzing the features that are present on the document to determine if it is authentic. You can see that this document would have been caught if presented at the border.

The CHAIRMAN. All right.

To Ms. Kephart, it looks pretty clear that something like this might have caused a little trouble for our Government Accountability Office investigators. Judging from what you have seen here today, do you believe that we need to install technology like this to help stop terrorists from doing what the Government Accountability Office did?

Ms. KEPHART. Well, Mr. Chairman, we know that terrorists thrive on forgery. They thrive on any variety of forgery they can use. So when you see something like this, which is efficient and effective, then it makes you believe that we can stop the forms of terrorist entry that involve forgery.

The CHAIRMAN. All right.

How likely, again, Ms. Kephart, do you think it is that terrorists or criminal fugitives trying to cross our border might try to bluff their way with a fake driver's license or other documents?

Ms. KEPHART. We know that John Allen Muhammad, criminal—whatever you would like to call him—used this as a primary means of getting into the United States for a number of clients. It would not at all be surprising that it has been a modus operandi for quite a while.

As I said in my oral statement, when I was on the Commission I was privy to information that indicated that we had quite a large number of terrorists residing here in the United States, and we did not know how they got in.

If we had watch lists in effect with passports, and these people were watch-listed, then how did they get in if they did not get in under an assumed identity or a fake document?

The CHAIRMAN. I would give all of you on the panel an opportunity to share some success stories where technology like this has been used and resulted in catching people using phony documents.

Mr. SHEPHERD. Sir, in my particular industry we have caught people using fake driver's licenses or credit cards who were trying to gain credit at the property. We have used that to try to prevent them from causing damage either to the property, financially, or to the people within the property.

The CHAIRMAN. All right.

Mr. CARR. Chairman Grassley?

The CHAIRMAN. Yes.

Mr. CARR. Our technology has been deployed in a variety of locations, including Departments of Motor Vehicles, for enrollment. I will give you two examples of where people have been caught. We have a particular State that has caught people on the terrorist watch list by using these kinds of technologies in the enrollment process.

We have another State that has deployed a system like what you have seen here today, where, in fact, illegal immigrants, within a day of hearing that this kind of document authentication has been deployed in an office, changed their pattern of application to move to other offices. This repeated over the course of five times, as different technologies like this were rolled out in those offices.

Mr. REEVES. Just to confirm; internationally, very recently, we were deploying in a pilot at a name-brand bank—I will not mention the bank—and this technology was available in the account opening part of the bank.

Within the first week, six fraudulent documents from very significant countries that one would be very concerned about, were found. After that first approximately 4 days, we found no false documents in that particular branch following that, exactly the same issue. This is a very organized process, and word gets out.

The CHAIRMAN. Because the word got out.

Mr. REEVES. Word got out that this branch can find bad documents. Very similar, a deployment at another bank, a pilot, in this country very close to where we are now, the common fraud is, someone will steal a good Mastercard check and then will make up a false document to match the identity on the Mastercard check. This was put in a high-crime branch, so we thought we would see a high level of fraud.

Literally, I believe it was the first day, possibly the second day, a person came in, tried to cash a check. It was a $5,000 check. When he saw what the teller was doing, going back and looking at this technology, literally ran out of the bank, left the check, left the card, and has never been seen since.

We have a number of systems deployed at one of our U.S. embassies. I do not want to disclose it for security reasons. I would be happy to share with the committee where it is.

It has been deployed and has run 25,000 to 30,000 applications for enrollment of new visas. The word from them, when we updated them for the purposes of this committee, was "we found hundreds of false documents." So, I think that is a very dangerous statistic.

The CHAIRMAN. Back to you, Mr. Reeves. It happened in June this year, I believe it was, that the father-in-law of a victim of the World Trade Center attack used a counterfeit Mexican Matricula card to enter the headquarters of the U.S. Department of Homeland Security here in this city.

Are you aware of any steps taken by the Department of Homeland Security in response to this incident? Have they looked at purchasing this type of scanner technology to protect the Department of Homeland Security Headquarters?

Mr. REEVES. We received an inquiry, I believe it was either the next day or 2 days following the publication of that event, which was very similar to this current GAO test. We had discussions with officials of DHS.

We also were asked for pricing. Initially we were asked for pricing for 2 units. We then were called back for pricing for 4 units.

We then were almost immediately called back for pricing for 6 units. Our understanding was that there are six entrance systems around their building.

We then received, from one of our re-sellers who re-sells our equipment as well, that they had been contacted as well relating to this same issue within a few days.

To the best of my knowledge, we have not actually received the purchase order, so in fact we have not actually sold these to DHS. But that is the status, as we understand it.

The CHAIRMAN. Well, it would seem to me, if they are thinking about doing it to protect their headquarters, it ought to be good enough then to protect our borders as well.

Now, I would like to get to something about cost. I recognize that you at the table may not have enough information to give us detailed price quotes today, but we asked you to provide some rough cost estimates in your testimony.

According to CBP, there are between 500 and 1,000 total inbound lanes at our ports of entry—that would be collectively, all over the country. According to a rough estimate you have given us, it looks like every lane could have technology similar to what we have seen here today for something in the tens of millions of dollars, in other words, a fraction of 1 percent of the Department's $35 billion budget.

Is that within the ballpark as any of you would see it?

Mr. REEVES. Well, I think Mr. Carr mentioned the number of $50 million being for fully deployed. That would be a system solution that would give you logging in of the crossing, as well as the technology to support it. I think my number was $2 million for the initial technology, with service costs running another $400,000 a year. So on a 3-year model, it would be about $3.2 million.

Rule of thumb would be that a fully deployed, integrated system would be 2 to 3 times that number, so that would take you to about $10 million on the outside for deployment of just the land borders. Of course, you would then have discussion on whether you migrated that to include the lanes in the airports and sea crossings as well.

The CHAIRMAN. All right.

Now, if there is no dispute over what he said, I will go on. I wanted to ask, is there any dispute there or anything to be added?

[No response.]

The CHAIRMAN. All right.

Then I will go to Ms. Kephart. If that would be about right, what kind of bang for the buck do you think that that would be in terms of catching, or at least deterring, terrorists and fugitives from using fake documents crossing our border? Would this be a good interim step to take before WHTI and the Real ID are fully implemented?

Ms. KEPHART. Well, you are talking about what I have always talked about, what we need to do to create effective and efficient borders. What we are talking about here, it seems to me, in watching the demonstrations, is that you have both effectiveness and efficiency built into this at a cost that is very low considering what you get for it.

We know that terrorists get shy very quickly when they think they are going to be caught. When I hear the stories here from the answers to questions about the deterrent effect it is having on banks, I cannot imagine that it would not have the same deterrent effect at our ports of entry.

The CHAIRMAN. Again, to anybody who wants to, but I am directing it to the whole panel, we heard from the Government Accountability Office that CBP failed to run name checks on their investigators, and they do not really have time to run name checks on every person crossing the border.

Would anyone like to explain how technologies like these could help CBP run name checks more often and more efficiently?

Mr. CARR. Mr. Chairman, our customers in the Departments of Motor Vehicles routinely use these kinds of technologies that both scan the document to authenticate it, but also reach out to databases to validate those kinds of identities, like the case that I mentioned where, by making that kind of a check, they were able to determine that the person standing in front of them applying for a driver's license was in fact on the terrorist watch list.

In this case, it was the Department of Public Safety, where not only did they refuse to issue the license, but they put the person in jail.

Mr. REEVES. Just to supplement that, I think one thing that may have been said, but may not be really obvious, is that the key to this kind of technology is the ability to read non-standard documents, so that when you are establishing and relying on building the entry or the record of that particular transaction, the ability to read non-standard documents is what really sets the technology apart and makes it universal.

Part of the services that are provided with the technology is the ability to enroll documents when, at a particular border or a particular entry point, new documents are being found.

That, in fact, is part of the technology, to vet those documents and build those and bring them into the library and the database so it becomes universal, so that any document being presented that the government is willing to accept, then can be part of this exit program, and then twice that number you would move it into an exit/entry system.

The CHAIRMAN. All right. Anybody else want to respond before I go to the next question?

[No response.]

The CHAIRMAN. Ms. Kephart's prepared testimony discussed the possibility of using real-time lost and stolen passport data from Interpol at checkpoints. I am wondering if this technology could work with that information.

Can anyone explain whether it would be possible, just as an example, to automatically read passports with these kinds of scanners, even if the passports were not originally designed to be machine readable, and then check their numbers against the list of known lost or stolen numbers?

Mr. REEVES. The short answer, if I could take that, Mr. Chairman, is, yes, this technology is already being used that way. Effectively, very often people are issued documents, passports, valid passports, in embassies. These passports generally are not standard from the standpoint of looking like every other passport that was issued in a passport office.

All of that technology, including the ability to enroll known fakes, the ability to enroll known stolen documents, can all be built into the system and it will not slow it down. It will operate at the same speed.

The CHAIRMAN. Anybody want to add? Go ahead, Ms. Kephart.

Ms. KEPHART. Well, just to discuss a little bit about Interpol's Lost and Stolen Passport database. That database right now has 100 countries enrolled in it, over 11 million lost and stolen passports in it. The case right now is that, at our ports of entry, that database of information, which can be downloaded real-time every 24 hours, is only available, still, in secondary inspection.

It would not be very hard to download that information into text, which is what primary inspectors check automatically when they do name checks, et cetera, and it is still not there.

So I have a little policy statement to make about the fact that it is still not available in primary. It would need to be available, I believe, in primary for these folks and their technology to be able to have access to it.

Mr. REEVES. Could I just, further, make one comment? In order to do this vetting, this data—the data generated by somebody presenting a document—can be put up to a trust authority. You do not even need this on the front line.

Privacy is something that can be dramatically improved by this type of technology, and using it against very important, well-maintained, secret trust authorities so that even that front-line border, or even the secondary border, does not have to have access to the actual information, merely the ability to ping that presented information back to that trust authority.

That privacy concern is really what we are seeing with various State legislators and other things. That is, their real beef with the Real ID Act is that really they are moving the data back and forth as opposed to vetting a particular identity and an identity document against that information, and if it checks out, then you know you have good information. So, privacy, I think, can also be dramatically benefitted, not demeaned, in using this type of technology.

The CHAIRMAN. Mr. Carr?

Mr. CARR. If I might, Mr. Chairman. The use of digital watermarking and other security features like this to authenticate the document is a means to make sure that that token that I am starting with, the document that I have been presented as an inspector, is, in fact, authentic. That can happen without compromising citizen privacy. The connections to a database can be made, if appropriate, within the context of policy and with security.

Today, with 35 million driver's licenses carrying watermarks and that number growing daily, from States that have really stepped out as leaders in innovating in security, like Iowa, which has added digital watermarking to the license, enhanced security features, and new document designs, we really do have tools that can aid in that front-line inspection to improve border security.

The CHAIRMAN. All right.

One last question, then. Again, to anybody, or the whole panel. Many of you are involved in working with State governments to help them comply with the Real ID Act and are knowledgeable about the progress towards implementing WHTI.

The administration says it will be ready and can implement both laws by their original deadlines in 2008. Would any of you like to describe your view of how ready our government is to start complying with these important security measures on time?

Mr. CARR. Mr. Chairman, I would like to comment.

The CHAIRMAN. You start out.

Mr. CARR. Thank you. What I would say is, Real ID is an opportunity to enhance the security of the driver's license, a critical identity document, across our Nation.

What is needed at this point are a set of well-defined standards that States can begin to implement against so that they know what is required of them to get from here to the implementation deadline.

Funding is also going to be required in order to allow them to implement the system upgrades and changes that are necessary to get there. Many States have moved out ahead of those decisions being made. Texas, for example, will introduce a new driver's license which incorporates state-of-the-art security that allows an inspector to both feel that the document is genuine, see that the document is genuine, and machine-authenticate it with technologies like digital watermarking.

So, in order to get to the deadline, we must address both standards and funding as a vehicle to move the States forward.

The CHAIRMAN. Mr. Reeves?

Mr. REEVES. Mr. Chairman, coming from the State of New Hampshire, the "Live Free or Die" State, the legislature in the State of New Hampshire made a stand, if you will, relating to a grant that was made available under the Real ID Act.

I could just not reinforce enough, as I have talked to the legislators—my wife is a legislator—that in the State of New Hampshire, the two issues that effectively became the controversial issues where this ended up getting tabled, whether or not to accept a major grant from the U.S. Government, was, one, they are saying these programs do not work; they ask us to do stuff and it does not increase our security.

The other part was, effectively, privacy. They are asking for more and more information, they have bigger and bigger databases, they are aggregating all this information. It is Big Brother.

Those two things, I think, are the report that I am receiving from the legislators in the State of New Hampshire, and I do not think they are unique. So I think, just for a comment, I think that is a big impediment with a number of the States.

As far as the fine tuning, I think if the privacy paradigm, some of the kinds of issues that are being dealt with by this committee right now, if they could be modified or impacted for Real ID, it would make a major difference in the State of New Hampshire. I will not speak for any other State.

The CHAIRMAN. Anybody else want to throw anything in at the tail end here?

[No response.]

The CHAIRMAN. Outside of thanking all of you and the previous panel for participating, I would say that we have also learned some really important things today. Of course, I am very disappointed with the results of the GAO study.

Not how GAO did it, because obviously they have demonstrated what we were hoping would not be the case, that it is easy to enter our country through the front door. But it looks like, particularly from this panel, that there are some workable solutions.

Of course, I hope there are people from the Department of Homeland Security who stayed behind. I do not know whether they did. I saw the people that were on the panel walk out afterwards, but it would have been nice if they could have seen this.

I hope that they learn something from this and that they would take some time to look at these tools that are available to help them in their job of keeping our country safe.

Now, in regard to the Western Hemisphere Travel Initiative, I think we heard today that that is very important. In fact, that is the basis for DHS not doing anything, because they are looking for the perfect way to do it, and that is that initiative.

I think we have to make sure that that is established on time. With that thought in mind, I am sending a letter to conferees of the Department of Homeland Security appropriation bill, requesting that they remove language from the Senate version which has the potential for indefinitely extending that deadline for the WHTI program.

We have heard that CBP thinks that this program is very important, and they are prepared to implement it by the deadline. I think it would be foolish to extend the deadline and then continue to keep the front door open. Obviously, we are all concerned about our Nation's security and maintaining strong, safe borders.

With that in mind, I think CBP should be on notice that this committee is going to continue to monitor their efforts. In fact, I am going to ask that CBP provide me with updates in what they are doing to fix the problem, and I would ask them to do that every 3 months until it is fixed.

I raised this point before. I do not want to be holding a hearing a year from now, or 2 years from now, and find out, as we did today, that there is nothing too much different in the situation, as evidenced by the measuring stick of the Government Accountability Office, from the way it was 3 years ago.

So you would hope that within a year, then, that the CBP failure rate would fall from that 93 percent that is demonstrated by this chart, down to 0 percent, which would be possible with this technological equipment. The driver's licenses used by the Government Accountability Office would have been exposed; we have seen that very clearly.

The record is going to remain open through close of business Friday, August 11. If Senators and staff who are here would like to submit questions for our witnesses, do so by that deadline.

Thank you all very much. I appreciate your testimony.

[Whereupon, at 11:50 a.m., the hearing was concluded.]

APPENDIX

Additional Material Submitted for the Record

Statement of
Jayson P. Ahern
Assistant Commissioner, Office of Field Operations
U.S. Customs and Border Protection
Department of Homeland Security

Chairman Grassley, Ranking Member Baucus, Members of the Committee, it is a privilege and an honor to appear before you today to discuss the U.S. Department of Homeland Security's U.S. Customs and Border Protection (CBP) and the recent Government Accountability Office (GAO) investigation of our ability to detect and interdict counterfeit state-issued driver's licenses and birth certificates.

I want to begin by expressing my gratitude to the Committee for the support you have shown for important initiatives that enhance the security of our homeland. Your continued support has enabled CBP to make significant progress in securing our borders and protecting our country against the terrorist threat. CBP looks forward to working with you to build on these successes.

On March 1, 2006, CBP marked its third anniversary. During this time, we have made great strides towards securing America's borders, facilitating legitimate trade and travel, and ensuring the vitality of our economy. As America's frontline border agency, CBP employs highly trained and professional personnel equipped with the resources, expertise, and law enforcement authorities to discharge our priority mission: preventing terrorists and terrorist weapons from entering the United States. Carrying out this extraordinarily important mission entails not only improving security at and between our ports of entry along the entire length of our land and maritime borders, but also extending our zone of security outward, beyond our physical borders.

Our efforts to gain operational control of our borders and push our zone of security outward enables CBP to better perform the traditional missions of its legacy agencies, which include apprehending individuals attempting to enter the United States illegally, stemming the flow of illegal drugs and other contraband, protecting our agricultural and economic interests from harmful pests and diseases, protecting American businesses from the theft of their intellectual property, regulating and facilitating international trade, collecting import duties, and enforcing United States trade laws. In fiscal year 2005 alone, CBP processed more than 29 million trade entries, collected $31.4 billion in revenue, seized 2 million pounds of narcotics, processed 431 million pedestrians, and passengers and 121 million privately owned vehicles, and processed 25.3 million sea, rail and truck containers.

CBP will take action to address the vulnerabilities identified by the recent GAO investigation into our ability to detect counterfeit documents. These notable actions will include:

- Delivery of 16 hours of basic fraudulent document training to all CBP Officers;
- Additional fraudulent document training to Counter-Terrorism Response Teams;
- Delivery of a series of musters designed to enhance awareness of and increase the detection of fraudulent identity documents;
- Installation of card reader technology in all land border primary inspection booths to allow faster and more accurate reads of machine readable documents, including U.S. passports;
- Increase in the use of name queries of law enforcement databases by primary inspectors at land border ports of entry;
- Purchase of identity checking guides for all ports of entry. These guides provide CBP officers with the basic security and verification features of all US and Canadian identity documents;
- Initiation of a program to increase CBP Officer training in state-issued identity document security features and validation processes. The CBP personnel who receive this document training will, in turn, train additional field personnel in their duty stations.
- Delivery of state-of-the-art fraudulent document workstations, which will provide CBP Officers with the latest in fraudulent, altered, and counterfeit document detection capabilities;
- Development of port-of-entry-specific strategic initiatives designed to increase enforcement and improve facilitation, including an initiative that leads us to verification of the identity of each applicant for admission and creation of a record of that person's travel;
- Development of targeting operations based on strategic methodologies allowing CBP to focus on specific groups, for example, those individuals who may present state-issued identity documents;
- Development of a web-based reference tool that will be made available to CBP Officers during primary inspection to assist in the verification of identity documents; and
- Development of an enhanced training package on establishment of identity to be delivered as part of the CBP Officer Academy and Post Academy training.

Addressing any major issue at the land border presents many challenges. The United States has over 7,000 miles of shared border with Canada and Mexico, and each day CBP Officers inspect more than 1.1 million passengers and pedestrians. This includes many who reside in border communities, who cross legally and contribute to the economic prosperity of our country and that of our neighbors. Maintaining this flow is critical; however, we must be confident in our determinations of who is crossing our border. In fiscal year 2005, over 84,000 individuals were apprehended at the ports of entry trying to cross the border with fraudulent claims of citizenship or false documents. Moreover, on an average day at our ports of entry, CBP intercepts more than 200 fraudulent documents, arrests over sixty people, and refuses entry to hundreds of non-citizens, a few dozen of whom are criminal aliens who are attempting to enter the United States. As the 9/11 Commission report stressed, security requirements governing travel to and from Canada, Mexico and parts of the Caribbean should be treated as equivalent to security requirements for travel to and from other parts of the world. Congress recognized this important principle when it passed the Intelligence Reform and Terrorism Prevention Act of 2004, which included what is now commonly known as the Western Hemisphere Travel Initiative (WHTI).

We realize the potential consequences that any changes to address these vulnerabilities could have on international travel. We are particularly mindful of the challenges presented in the land border environment, where approximately two percent of travelers crossing the border are responsible for nearly 48 percent of all cross-border trips, and the cross-border relationships and cultures are vibrant and dynamic.

However, just as passenger behavior in the commercial airline industry has changed since the terrorist attacks of 9/11, travelers within the western hemisphere must also become accustomed to possessing authorized travel documents when crossing our borders. That some individuals currently can cross the border without verifiable documents, or without any type of travel or identity documents in their possession, is a significant vulnerability to our national security.

The standardization of travel documents is a critical step in securing our Nation's borders. Currently, there are thousands of different documents that a traveler can present to CBP Officers when attempting to enter the United States, creating a tremendous potential for fraud. Standardization of documents will eliminate the time-consuming, manual process of reviewing and validating a host of distinct and sometimes illegible and unverifiable birth certificates and other identity documents. The use of standardized documents that will enable automated reading and vetting of the information will also be essential to achieving the facilitation benefits of WHTI; valuable time is wasted and accuracy is reduced if manual data entry is required in order to perform necessary database and watchlist queries of passengers. Automated reading and vetting of identity documents will also be an important tool for CBP in distinguishing the small set of incoming travelers who pose a potential threat from the legitimate traveling public.

In addition to determining the appropriate documentation under the WHTI, the Department of Homeland Security (DHS) and the Department of State (DOS) are also carefully examining the best type of technology available to enable CBP Officers at the border to quickly and automatically, with appropriate privacy protections validate a traveler's identity and citizenship. Standardized and automated travel documents will enable us to efficiently, reliably, and accurately identify a traveler and his or her citizenship without having to review an assortment of documents and pursue an extensive line of questioning thereby facilitating travel.

Existing "trusted traveler" programs are also being evaluated for expanded use at our land borders. These include the Secure Electronic Network for Travelers Rapid Inspection (SENTRI), Free and Secure Trade (FAST), and NEXUS programs. These programs facilitate the crossing of low-risk, frequent travelers and commercial truck drivers at the land borders, through exclusive, dedicated lanes. To enroll in these programs, travelers must provide proof of citizenship, a Border Crossing Card (BCC) or visa, if required, as well as other identity documentation, such as a driver's license or ID card. An intensive background check against law enforcement databases and terrorist indices is required, and includes fingerprint checks and a personal interview with a CBP Officer. To date, approximately 225,000 SENTRI, NEXUS, and FAST cards have been issued. Over the next few months, we expect to increase the number of locations where they can be used. These programs are implemented in partnership with the governments of Canada and Mexico, and include the participation of many citizens of these countries. In light of the extensive background checks and pre-vetting of enrollees in these programs, we are evaluating whether the presentation of a trusted traveler card when traveling through the dedicated NEXUS, SENTRI or FAST lanes can serve as sufficient evidence of a traveler's identity and citizenship for purposes of meeting the requirements of WHTI.

To ensure that affected stakeholders will be able to convey their comments and concerns about WHTI, we are using a robust rulemaking process that allows multiple opportunities to comment. In addition, we have attended over 30public sessions and town hall meetings and DHS representatives have met with 670 community leaders and stakeholders to discuss this initiative. We are committed to continuing to work with affected stakeholders to mitigate potentially adverse effects as this initiative gets underway.

Given the magnitude of change this initiative will entail, DHS and DOS, in consultation with other government agencies, have proposed a two-phased implementation plan for WHTI. This approach was outlined in the Advanced Notice of Proposed Rulemaking (ANPRM), which was published in the Federal Register on September 1, 2005, and had a 60-day public comment period. In response to this advance notice, approximately 2,000 public sources, including governors, mayors, police chiefs, tribal leaders, business leaders, and border community members submitted comments. Both DHS and DOS recognize the unique issues that this initiative will raise, and we will remain flexible when working with affected entities and communities.

WHTI is an essential element of our layered approach to security at our borders. DHS and DOS will use our resources to implement this travel initiative by the deadline set forth in law. However, this is just one step in our ongoing efforts to secure our borders. We are making substantial progress every day--through our Secure Border Initiative (SBI), which is a comprehensive approach to border security, through enhanced border security task forces, and in a host of other ways.

We will also continue to work with Congress in support of the President's call for comprehensive immigration reform that is necessary to increase border security and interior enforcement and that creates a temporary worker program and addresses the problem of the estimated 11 to 12 million illegal immigrants already in the country.

Mr. Chairman, Members of the Committee, I have outlined today some of the issues that we are faced with in attempting to ensure identification and verification of citizenship of each applicant for admission.

CBP will continue to protect America from the terrorist threat while fulfilling our other important traditional missions. But our work is not complete. With the continued support of the Congress, CBP will succeed in meeting the challenges posed by the ongoing terrorist threat and the need to facilitate ever-increasing numbers of legitimate trade shipments and travelers. Thank you again for this opportunity to testify. I would now be happy to answer any questions that you may have.

Statement of Senator Max Baucus
Hearing Before the Senate Finance Committee
Border Security Oversight
August 2, 2006

A little over a month ago, Canadian authorities raided several Toronto-area buildings. Police arrested Canadian Muslim men and boys. And police seized 3 *tons* of the explosive fertilizer ammonium nitrate.

That's enough for three giant truck bombs. And each of those truck bombs could do major damage to a high-rise building. The government believes that it caught a "home-grown" terrorist cell, intent on blowing up targets in southern Ontario.

Illegal immigrants challenge our southern border. But would-be terrorists challenge our northern border.

Our 4,000-mile border with Canada has long been a source of pride and prosperity, as the world's longest demilitarized border. But now those 4,000 miles pose one of our nation's greatest security challenges.

We need to get border security right. Tight security along our Nation's border is critical in the war against terror.

And in terms of border security, GAO's testimony today is, in a word, *alarming.*

It's one thing for the Customs and Border Protection agency to fail to imagine a security problem. But it's quite another thing to actually be warned about a problem and fail to fix it for 3 years. The Senate Finance Committee publicly raised these very border security concerns in a 2003 hearing. But now, 3 years later, a follow-up GAO investigation reveals that the same vulnerabilities continue.

GAO investigators designed fictitious driver's licenses and birth certificates. They used off-the-shelf graphic software, available to any purchaser. And then they tried to enter America.

GAO's investigators tried to enter America 15 times using counterfeit driver's licenses and an expired, altered U.S. diplomatic passport. For some entries investigators used the same driver's license and birth certificate that they used in the investigation 3 years ago.

At two border stations, one in Arizona and one in Texas, INS officials did not ask for *any* identification document when GAO investigators entered the United States.

During 11 other attempts, the investigators presented counterfeit documents. And Customs and Border Protection officials waved them through.

We saw some progress. In New York and Florida, GAO investigators were detained after presenting counterfeit IDs. But batting .130 is not good enough, even in baseball. And it's certainly not good enough in the war on terror.

I have worked hard to bring more Customs and Border Protection personnel to the Montana border. And we have amended the Homeland Security appropriations bill to pave the way for unmanned aerial vehicles on the northern border. We need these

UAVs because of the length of the border and the amount of wilderness, ranch, and farm land lining the border. It's almost impossible to patrol this border on foot, in cars, or on horseback.

But ports of entry are different. There, Customs and Border Protection agents *are guaranteed* a chance to *look people in the eye* and check their documents. Our border personnel need to work harder and smarter to spot forged documents.

I expect to hear today that everything will be fine when the Western Hemisphere Travel Initiative card—the WHTI card—is developed. But the Senate just passed a Homeland Security Appropriations bill that delays the card's introduction date for up to 17 months—to June 1, 2009. The Homeland Security Department and the State Department are fighting over its design.

It's fine occasionally to point to a solution down the road. But in the fight against terrorism, that could be a deadly mistake.

Almost 5 years have passed since 9/11, without another terrorist attack on American soil. Some things have gone right. Hard work of law enforcement personnel has made a difference. But that does not mean that we can relax. It means that we need to redouble our efforts.

That means getting the job done to identify false documents presented at the border.

I strongly urge the administration to quickly complete the task of developing a plan for secure documents.

I'm pleased that we will also hear today from companies that are in the business of developing document-checking systems. I hope that their testimony will help us to think through whether a driver's license based system is a solid option for enhancing border security.

We will hear that the technology exists for border personnel to take 3 to 4 seconds to check a person's driver's license. It may make more sense to develop this system than to rely on a controversial and hard-to-implement WHTI card. This system could be both secure and efficient. And this could be a solution that does not interrupt the flow of goods and services between the U.S. and Canada.

I want to thank the GAO for their hard work on this investigation. And I want to thank Chairman Grassley for keeping the Finance Committee focused on this critical issue of border security.

We need to get border security right. Lives depend on it. And hearings like this are part of the answer.

DIGIMARC

Prepared Testimony by Scott Carr
Executive Vice President, Digimarc Corporation

U.S. Senate Committee on Finance

"Border Insecurity, Take Two: Fake ID's Foil the First Line of Defense"

Washington, D.C.
August 2, 2006

Executive Summary:

Digimarc is the leading supplier of government-issued citizen identity documents in North America. Our systems are used to enroll citizens and issue more than 2/3 of all U.S. driver licenses. We supply similar systems for production of the Mexican voter identification documents and driver licenses in several Canadian provinces.

Customs and Border Protection and law enforcement officers face extraordinary challenges as they try to authenticate the more than 200 forms of valid driver licenses circulating in the U.S. today through unaided visual inspection. This testimony discusses technological innovations that are available now and in use by several State governments and commercial entities to augment visual inspection of driver licenses. Such technologies, like digital watermarking, are already in broad distribution, and can be used to machine authenticate U.S. driver licenses, travel documents and other modern identification documents. Solutions, like those demonstrated today, could be leveraged by the Federal government to improve the security of our borders within 6 to 12 months.

Although many States are engaging in impressive innovation in driver license security, we will pay special attention today to a Department of Transportation pilot study conducted by Nebraska that is right on point with the concerns of the Committee. This pilot study, coupled with the investments that Nebraska has made in identification security, provides a useful case study to inform the national debate about the use of driver licenses for crossing our land borders with neighboring nations. A demonstration of readily available solutions that can machine validate identification documents is provided, as are a number of public policy recommendations that seek to contribute to implementing effective strategies to protect our homeland.

DIGIMARC

Introduction:

Chairman Grassley and Ranking Member Baucus, I would like to thank you both, and your colleagues on the Finance Committee, for giving me an opportunity to appear before your Committee to provide a demonstration of technologies that can be deployed right now to help better secure our borders. The technologies I will describe are not some futuristic ideas being built in a lab but are currently in use and ready for full-scale deployment.

I am appearing before your Committee as an expert in the field of secure ID solutions. As an Executive Vice President at Digimarc Corporation, I have responsibility for product marketing, business development and product development for Digimarc's secure identification solutions. In my 10 years with Digimarc, I have held a number of executive management positions leading the development and successful deployment of digital watermarking and government-oriented document and ID security applications.

Digimarc Overview:

Digimarc has been in the business of supplying issuance systems for driver licenses and other government-issued credentials for nearly 50 years. Our company is the leading supplier of government-issued IDs in North America and also supplies similar products and services in more than 20 foreign countries including Mexico, Haiti, Russia and the United Kingdom. We are also a trusted supplier of a global system used by an international consortium of central banks to deter digital counterfeiting of banknotes.

Our company's systems issue more than 60 million identification documents annually, and are employed by 32 U.S. States and the District of Columbia, producing more than 2/3 of all driver licenses issued. We support the States with solutions that cover all aspects of ID issuance including applicant identity verification and enrollment, over-the-counter and centralized secure card production systems, design and manufacturing of the cards using advanced technologies and multiple security features, and inspection to authenticate the ID after it has been issued. To date, Digimarc provides centrally issued driver licenses to 12 States, comprising about 80% of all centrally issued IDs in the U.S.

Additionally, Digimarc pioneered a signal processing technology innovation known as "digital watermarking," which allows imperceptible digital information to be embedded in all forms of media content, including personal identification documents, financial instruments, photographs, movies, music and product packages. In identity documents digital watermarking is used to embed digital data within the structure of the document that is imperceptible to the human eye. It creates a machine-readable security feature that links together numerous elements of the document allowing machine authentication to readily identify counterfeit and fraudulent documents.

At the point of inspection digital watermarks can be easily detected and read by a number of commercially available devices, including document scanners, PDAs with built-in cameras, mobile phones and other digital devices. A quick scan by an authorized reading device, equipped with special software, analyzes the information embedded in the digital watermark as well as other information contained in security features present on the document. This enables the immediate detection of photo swapping, altered data or re-originated documents – the primary forms of counterfeiting.

U.S. Driver License Security Enhancements:

U.S. States began incorporating digital watermarking in their driver licenses in 2002 using a Digimarc product known as Digimarc® IDMarc™. Eighteen States have adopted this important security capability in their driver licenses, including key border States such as Washington, Michigan, Minnesota, Florida, Texas, and Vermont. In Michigan, for example, more than 75% of circulating licenses contain a digital watermark that could be authenticated at the U.S. / Canadian border. A number of other significant border States have also adopted digital watermarking, but they have chosen to keep their participation in this program confidential for security reasons. Examples of States in other areas of the country that have adopted digital watermarking include Iowa, Wyoming, Nebraska, New Jersey, Kansas, and Massachusetts.

Incorporated today in more than 35 million circulating driver licenses, digital watermarking is a covert, machine-readable feature that enables reliable cross-jurisdictional authentication of U.S. driver licenses. By the end of the year, 1 in every 3 issued driver licenses will include digital watermarks and this number is growing rapidly.

Digital watermarking complements other authentication techniques such as the pattern matching and multi-spectral analyses found in passport and travel document scanners. Digital watermarking technology is compatible with and can enhance the security of passports, smartcards and other travel documents such as the proposed PASS Card. Digimarc broadly licenses digital watermarking technologies to many other vendors for supply of digital watermarking enhanced solutions for a variety of security purposes.

Deployment of digital watermark reading is aligned with the published security strategies of the Department of Homeland Security and the Department of State, and is a recommended feature of the Document Security Alliance and an approved optional feature of the HSPD-12 PIV-2 standard, which calls for enhancing the identification and authentication of federal employees and contractors. Digital watermarks provide positive document authentication, age verification, cross-jurisdictional authentication, and forensic capabilities.

Our Insecure Borders:

Until recently, inspectors at air travel ports of entry had relied solely on reading an OCR strip on the bottom of a passport to identity the document. Upgrades to these systems have introduced "full page" readers that now use pattern recognition and remote databases to validate the document and the card holder. Similar investments have not yet been made to enhance driver license inspection across the U.S. land borders. Features, like digital watermarking, exist today in driver licenses that could allow improvement in inspection of driver licenses to progress as has been the case for passports, yielding a substantial improvement in security and crossing lanes.

Since Sept. 11, 2001, the United States Government Accountability Office (GAO) has published a number of studies that have demonstrated how insecure our borders really are. In 2003, and also as described in today's testimony, GAO officials partnered with agents of the Office of Special Investigations to develop counterfeit documents. These were used by special agents to enter the United States from various ports of entry from the Western Hemisphere. In GAO's most recent series of tests, 17 of the 19 counterfeit driver licenses were produced by using off-the-shelf, commercially available graphics software, a computer, a scanner and a printer, and were successfully used to cross into the United States. Our hard-working border officials were unable to detect these fakes because they do not have all the tools they need to properly verify the authenticity of these types of documents.

Visual inspection of travel documents—the key method our inspectors have today – is inadequate for a number of reasons, including the fact that there are more than 200 valid U.S. driver license formats. Only specialists, with years of training, have the skill sets needed to conduct reasonable visual inspections, and even then, visual inspection alone is not adequate to catch digital counterfeits. Our border agents do not have the necessary training or tools to inspect these documents on a day-to-day basis at ports of entry. This is made more difficult by the demands that arise from timely processing of thousands of individuals every day. Machine-authentication of the digital watermark present in these documents would take the guess work out of determining which documents are valid and which are not.

As noted below, the positive results from the U.S. DoT / Nebraska digital watermarking pilot confirms that viability and applicability of digital watermarking on U.S. driver licenses to aid in quick, reliable machine authentication at the U.S. border.

DIGIMARC

Leveraging State Investments in ID Security to Secure our Borders:

States have made and are making major investments in their driver licenses and issuance systems to promote transportation safety, protect their citizens from identity theft and fraud, and enhance their personal security and the security of the nation. As we know, the perpetrators in the Sept. 11 terrorist attacks obtained valid driver licenses under false identities. In any security system, criminals tend to look for weak points to exploit. In these cases, the documents were genuine driver licenses obtained fraudulently. The States and their suppliers are upgrading not only the documents but also the enrollment process and inspection processes to address all know weaknesses that could be exploited by criminals. According to the National Conference of State Legislatures, the States are expecting to invest billions of dollars as they continue to enhance the security of their driver licenses in compliance with federal standards being established to implement the REAL ID Act. These efforts will result in a citizen ID infrastructure that will deliver a high level of security in the enrollment, issuance and inspection processes. The States have established security processes that complement and extend many of the steps that are used for the current passport, or expected PASS card.

The processes and technologies being deployed by the States could also be used to strengthen the enrollment processes for Federal employee credentials and citizen credentials such as Passports, and can be used in conjunction with gaining citizenship certification from Department of State for State-issued REAL ID-compliant driver licenses. These improved enrollment processes include:

- Secure in-person photo capture to protect against fraudulent photo submittal and enable downstream biometric facial recognition
- Electronic scanning and archiving of documents enabling efficient enrollment, subsequent forensic investigation of documents, and electronic transmittal as part of adjudication process
- Electronic document authentication at point of enrollment using a variety of machine readable features including digital watermarking
- Electronic applicant verification against federal and third party databases such as Social Security
- Electronic verification of applicant data against State DMV and vital record databases
- Facial and/or fingerprint recognition, both 1-to-1 and 1-to-many, to verify identity against existing biometric records

- Use of trained driver license agency personnel who are experienced in fraudulent document recognition, work with enrollment processes on an ongoing basis, and have successfully passed thorough background checks

Leveraging Existing Technologies to Secure our Borders:

As described above, proven, cost-effective technologies are commercially available today that can enable border officials to machine authenticate U.S. driver licenses. These documents contain numerous security features such as digital watermarks, holograms, and special inks. There are software and hardware solutions available that can automatically inspect such security features and facilitate background checks via third party data bases. Digital watermarks are key in that they provide the only means in use today of trusted authentication of a driver license, and can be read using commercially available scanners and special software.

In addition to applicability in detecting and deterring ID counterfeiting, digital watermarks are a proven layer of security in global efforts to protect banknotes from digital counterfeiting. We have a multi-year contract with an international consortium of Central Banks in which we have developed and deployed, and are supporting and continuing to enhance a system to deter digital counterfeiting of currency using personal computers and digital reprographics. Work on the system began in 1997. Further details of the system are confidential for security reasons, yet it is important to note that digital watermarking is a proven and widely deployed security technology in such other anti-counterfeiting initiatives.

Digital watermark-based document authentication solutions are compatible with other travel document reading efforts including the ePassport efforts. This capacity to work with an ever-evolving set of security features is essential because it ensures that our government can stay ahead of terrorists and criminals who seek to use loopholes in our security systems to gain access to our country. Additionally, these technologies can be quickly deployed, within 6 to 12 months, and are efficient for the inspector to use so that citizens are not inconvenienced with long lines. And essential to success, digital watermarks do not compromise citizen privacy.

Summary of Nebraska ID Authentication Pilot Results:

Today, I will demonstrate a few examples of these technologies. But first, I would like to discuss what one State, Nebraska, has already done to raise the ID security bar by deploying innovative security solutions and processes. The experience of Nebraska, and similar experiences in several other States that have implemented driver license security innovations, can be leveraged by the

Federal government to help make our nation's borders more secure in a timely and cost effective way. Iowa, for instance, has deployed secure card materials, digital watermarking, and many other cutting edge solutions. The State employs fulltime investigators to attack license and identity fraud, and has deployed advanced readers to help officials detect counterfeits.

In 2003, Nebraska was one of the first States in the country to incorporate the digital watermarking feature into its licenses. Today, more than 60% of valid driver licenses in Nebraska are secured with digital watermarking, and Digimarc anticipates within two years all valid Nebraska licenses in circulation will be protected by IDMarc.

In 2005, the Nebraska Department of Motor Vehicles conducted a pilot under a grant from the U.S. Department of Transportation to demonstrate authentication of digitally watermarked driver licenses as a means to fight ID counterfeiting, reduce the purchase of age-restricted products, such as alcohol, and enhance traffic safety.

Digital watermark scanners were installed in a total of 18 point-of-sale sites, 30 office sites, and 35 law enforcement sites, and were used in "real time" for an average of 30 days The deployed readers continue to be used by the state, and in fact, this summer, Nebraska plans to put new Digimarc Document Inspector units into production at DMVs across the State. This will arm front-office operators with the tools to inspect and positively authenticate the millions of U.S. driver licenses secured with Digimarc IDMarc digital watermarking. Authentication will take place when Nebraska and other State driver licenses are presented as proof of identity to obtain a new or renewal driver license. This includes licenses from neighboring States such as Colorado, Iowa, Kansas and Wyoming – effectively removing the guesswork that can come with visually inspecting an out-of-state ID.

At the conclusion of the pilot, Digimarc staff interviewed the users regarding their experience with and response to the digital watermarking technology. Retailers, law enforcement and DMV operators were equipped with reader devices that allowed them to verify the information printed on a driver license—even an unfamiliar out-of-state driver license—against the information contained in the digital watermark. By doing so, they were able to determine if a driver license was valid or not and in the retail situations which, if any, age-controlled products the DL holder was old enough to purchase. The scanner/reader devices proved invaluable in instantly determining whether or not the license presented was authentic, as well as validating the age of the DL holder.

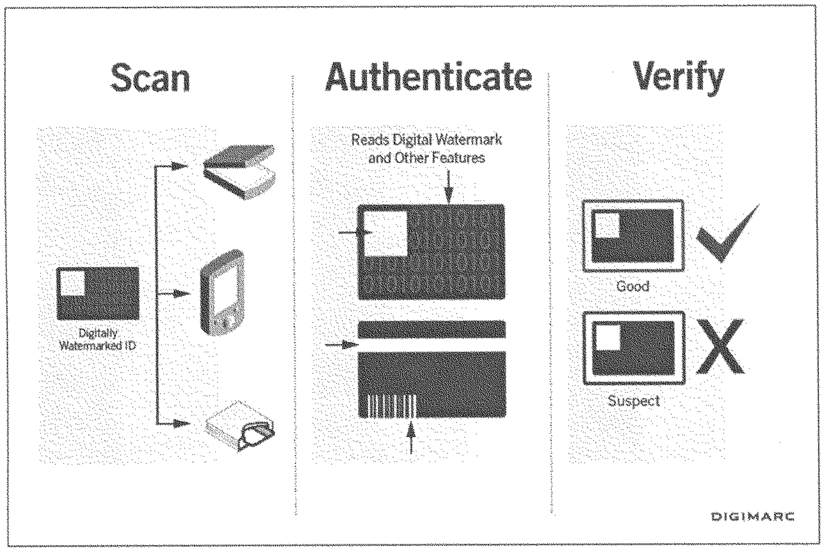
- 100% of retail participants said that a valid read from the watermark gave them confidence that the DL was authentic.

- 100% of law enforcement participants using a PDA reading device had confidence that a valid read from the watermark meant the DL was authentic.

- 100% of office staff surveyed reported that they believed the device was beneficial, that it gave them confidence that the scanned ID was authentic, and that they would use it in the future.

Digimarc Document Inspector Demo:

Authenticating documents like driver licenses and IDs can be done quickly and simply with a single device that scans both sides of the document simultaneously, and the Digimarc Document Inspector software that checks the validity of common ID security features, including the digital watermark.



I have two Nebraska driver licenses. The names and demographic data on each are the same. The cards visually appear to contain all the same security features. But the two photos are different. Thus one must be a fake.

I will start by inspecting one document by inserting it into the scanner. The software is very easy to use – the operator just hits the spacebar to initiate the scanning process.

DIGIMARC

In just a few seconds, the device scanned both sides of the document and the software processed the information, determining that the document is authentic for that document type and jurisdiction. The software contains a regularly updated document information library that is used for this automated validation process.

The software read the individual's demographic data from the document to display to the operator, which assists validation of the document and card holder. This entire process produced a valid rating in seconds, displaying "green" clearly on the screen so it's easy for the operator to see it passed inspection – enabling them to focus on the individual, rather than the document.

Now I'll scan the second document. To the human eye, this Nebraska license looks identical to the previous "valid" one I just scanned, and would pass any manual inspection by a border agent.

The scanning process was the same, only the result was a clear red indicator on the screen that the document is suspect. This counterfeit was made by swapping a photograph from a driver license produced in a different State, and placing it on this Nebraska license. The software was able to determine the mismatch and flag the document as suspicious for the operator to take action or conduct further investigation. In a typical border crossing scenario, this card holder would be sent to secondary inspection where an investigator could use the digital watermark and other features or databases to pursue the fraud.

Digital watermarks can also be read and authenticated on travel document scanners, like the kind used to read passports. Here, our software is able to draw on the pattern matching library of such a scanner and its multi-spectral light inspection authenticate the watermark and check additional security features visible only when illuminated in UV or IR light. This is a more expensive solution, but one that can validate not just driver licenses and IDs, but travel documents like passports and foreign ID cards.

For example, if I insert a genuine Massachusetts driver license first into the barcode/magnetic stripe reader device read data from the 2D barcode on the back of the document you'll see the individual's demographic data from the document display on the screen, but the document rating is "Pending". I can now scan the front of the document on the travel document reader and the software processes the information, determining that the security features are authentic for that document type and jurisdiction. In this example, the digital watermark and document design and format features for a Massachusetts driver license of this particular series year were all authentic. Like in the previous demonstration, the software contains a regularly updated document library that is used for this automated validation process.

DIGIMARC

The Digimarc Document Inspector closes the loop on the secure ID lifecycle by providing an easy, reliable way to instantly authenticate IDs after issuance. Border inspectors can immediately validate the document using the digital watermark and other data and features present on the license. Visible features, like 2D barcodes and others, can be altered, but when linked to a second feature that is imperceptible to the human eye, counterfeiting becomes extremely difficult, if not impossible. After scanning, Document Inspector provides a quick pass/fail reading and keeps lines moving.

Digimarc Document Inspector is fast and easy-to-use. An operator can authenticate a document with confidence in just a few seconds. Our software is hardware independent, working seamlessly with a variety of best-of-breed hardware and software components, and provides a simple user interface to eliminate the guess work associated with visual inspection.

Document Inspector can validate a deep set of security features. Depending on options selected this includes an extensive database of U.S. driver license security features such as barcodes, magnetic stripes, document layout features in visible light (placement, size), and features in UV and IR light. The database is updated on a regular basis, and updates can be distributed in multiple ways.

Table 1 summarizes the Document Inspector features and benefits.

Table 1 Digimarc Document Inspector Features and Benefits

Features	Benefits
Extensive document database that is updated regularly	• Standardizes authentication practices • Gives agents more confidence • Keeps the knowledge base up to date without the need for additional training •
Fast, easy authentication results	• A clear red/green indicator of authentication evaluation • Multiple visual cues to the result • Ability to see the details if further investigation is necessary •
Standards-based technology	• Allows for integration with external systems • Keeps deployment/investment costs low • Provides clear technology path

In summary Digimarc Document Inspector is a document authentication solution that features:

- A system that offers fast document authentication to ensure citizens are not inconvenienced or slowed down by the process.

- Authentication of the most comprehensive set of security features used in driver licenses

Cost Estimates of Deploying Readily Available Technologies:

Digimarc does not have access to all of the government information, including technology integration, human resource, and third-party database expenses, to offer a precise estimate of what it would cost the Federal government to deploy these readily available technologies to help secure our borders. We respectfully suggest that the Committee request that the Congressional Budget Office or the Office of Management and Budget conduct such a study.

It is our understanding that the number of Northern and Southern land border points of entry are:

	Inbound Passenger Lanes	Inbound Cargo Lanes	Pedestrian Lanes	Total Lanes
Northern Land Border POEs	278	121	24	423
Southern Land Border POEs	224	72	86	382
Total	502	193	110	805

Our own rough estimate of the cost – based on our experience and market research studies – of deploying the necessary software and hardware in an estimated 805 lanes to cover all immigration land border lanes, including cargo and shoulder lanes is under $50 million. This would equip each lane to machine validate driver licenses and other common travel documents. Covering the Northern border lanes, assuming 423, the cost is approximately $26 million. If we wanted to add any type of remote database interface to this system such as cross referencing watch list databases or consolidating the number of transactions etc. we would add an additional $10 million to our baseline cost estimates.

These cost estimates do not include the cost to the States of deploying machine-readable security features, nor do they capture the expense to the States of improving a large number of their security programs such as their enrollment processes. But these requirements have already been mandated by the REAL ID Act and the States are already working out how to pay for compliance with this Act. In any case, if our cost estimates are roughly in the ball park, this would be a small price to pay to quickly improve the security of our borders.

Public Policy Recommendations:

We recommend that the Federal government promptly deploy capabilities to machine verify the authenticity of U.S. driver licenses at the border, including reading and authenticating the digital watermark. Over time, these readers could be upgraded to accommodate enhancements being made to driver licenses and other identity documents from both the U.S. and Canada, and also other from other Western Hemisphere countries as deemed appropriate by the Department of Homeland Security and the Department of State. These technology solutions are scalable, having the capacity to integrate new technologies that will be developed in the future to ensure that criminals and terrorists are always challenged to defeat ever higher levels of security.

Every border crossing official must be able to do machine-readable verification of driver licenses, processing the covert machine readable features in documents that are presented at the border. In addition to putting stationary readers at all border crossing stations, mobile readers should also be deployed to ensure that agents can do rapid and secure screening of driver licenses and/or travel documents. This will help ensure that transit times are not unduly affected.

All of these technologies exist today and are proven, and could be deployed in 6 to 12 months if the funds were available. Even if the U.S. government implements new border crossing mandates in the future so that only passports are to be utilized for border crossing, a position which we disagree with as described below, such a deployment would provide additional security before that date and also could ensure the integrity of the proposed PASS cards.

The REAL ID law requires the States to add a machine-readable feature to their driver licenses. Given that digital watermarking has become a de facto standard for driver license authentication, we recommend that the Federal government require or encourage all States to adopt digital watermarking technology in addition to other appropriate machine-readable security features to comply with the requirements of this law so that national standard authentication will be realized.

We likewise urge Congress to help the States pay for REAL ID compliance. The REAL ID Act will help States meet the security challenges of the 21st century by ensuring that they deploy best-of-breed, end-to-end security systems. Given the cost—initial cost estimates by the National Conference of State Legislatures suggest that compliance will run between $9 and $13 billion--the Federal government should not impose a large unfunded mandate on the States to meet our national objective of protecting our homeland.

Finally, we recommend that Congress harmonize the Western Hemisphere Travel Initiative and the REAL ID Law. After two years of debate, the State Department and the Department of Homeland Security continue to grapple with the development of technical specifications for the proposed PASS card that is designed to implement WHTI without crippling cross-border commerce. In light of concerns with the ability of the government to have the structures in place to implement WHTI at the end of next year, the Senate recently passed amendments to the Immigration and Homeland Security appropriations bills that would delay the implementation date for WHTI by 18 months. Senators expressed concern about the impact of this program on economically significant cross-border travel and tourism given the high per card cost of the credential to citizens and questions about whether citizens will know they have to obtain a new credential to cross a land border. Senators also expressed doubt as to whether these Departments will be able to set up a new program in an efficient and cost-effective manner. Given the uncertainty associated with the PASS program we advocate that Congress insist that willing States be allowed to issue REAL-ID compliant driver licenses that would be an alternative to the PASS card for WHTI compliance. We recognize that the Departments have no choice under current statutory law but to try to find a convenient solution that can be ready at the end of 2007, but Congress has the ability to authorize and fund an equally-secure, more-convenient alternative for millions of American citizens.

This approach would leverage the significant investments in ID security that the States have already, and will continue to make, in the coming years, and would require DHS to establish a common standard of technical standards to be applied to any credential used for land border crossing. This approach would also leverage the existing ID systems that the Canadian Provinces have already deployed. The opportunity for both the United States and Canada to develop a collaborative approach should not be missed.

Conclusion:

In conclusion, I would like to thank Chairman Grassley and Ranking Member Baucus for giving me the opportunity to appear before the Finance Committee on behalf of Digimarc Corporation. Speaking on behalf of the community of issuers that we serve, and the citizens of our nation, we want to express appreciation for this Committee's support of the work of the Government Accountability Office, and its inspectors in challenging our government agencies to do the best possible job they can to secure our borders.

The States have been pressing forward with important security upgrades within the limits of their budgets and mandates. More will need to be done as States drive to comply with the REAL ID law. It makes sense, therefore, for the Federal government to leverage these significant investments to help secure our borders, and at the same time, save tax payers money and time in obtaining identification credentials. Digimarc Corporation, along with other suppliers and the many of the issuers that we serve stand ready to do all we can to support the government's objective of enhancing the security of our homeland.

Digimarc Corporation Government Programs Case Study

U.S. Department of Transportation and Nebraska Department of Motor Vehicles

In our increasingly fast-paced, technologically-advanced, Internet-connected world, identity theft and fraud impact nearly all segments of our lives, from personal security to the threat of terrorist activity, to highway safety.

According to a 2006 Federal Trade Commission report, consumer complaints of identity fraud and theft increased 25% between 2003 and 2005[1], with total economic losses to consumers of approximately $5 billion and a total cost to businesses of over $48 billion.

The most recent statistics available from the FBI state that domestic terrorism cases increased from almost 3,500 in 1999 to more than 6,000 in 2003. A chilling FBI report[2] sites a case of a package intercepted by the FBI that contained half-a-dozen fake identity documents—all in different names but with the same picture—along with a stash of deadly chemicals and instructions on how to turn them into poison gases.

Finally, a recent report[3] from the National Highway Traffic Safety Administration revealed that in 2004, 24% of drivers between the ages of 15 to 20 who were killed in traffic crashes had Blood Alcohol Content levels of .08 or higher. While traffic crashes and fatalities are the most visible dangers of underage drinking, alcohol consumption by minors is also associated with increased rates of violence, suicide, unsafe sexual behaviors, fetal alcohol syndrome, and educational failure. The social cost of underage drinking has been estimated at $53 billion; this total includes $19 billion from traffic accidents and $29 billion from violent crime. The monetary impact in terms of increased health risks and diminished prospects for future success are incalculable.

Any way you look at it, identity theft and fraud is a huge and ever-increasing problem. The reasons for the increase in identity theft and fraud and the use of false IDs can be directly attributed to current technology in digital imaging and printing, and the increased use of the Internet for information exchange and multimedia content sharing. High quality color printers and copiers have made false IDs easier than ever to fabricate, and the Internet provides ready access to hundreds of vendors who sell ready-made false IDs online. These two technological advancements have made it progressively more difficult to reliably authenticate IDs through simple visual inspection. Machine readable authentication at point-of-inspection has, thus, become essential to secure identity credentials.

To provide machine readable authentication and aid states in the fight against ID counterfeiting, fraud, and theft—whether by minors or adults—Digimarc developed the Digimarc® IDMarc™ digital watermarking security feature and began offering it to driver license agencies in 2002. Incorporated today in more than 25 million driver licenses, IDMarc is a covert, machine-readable digital watermarking feature that enables cross-jurisdictional "turn-key" reading and authentication of state-issued identity documents, including driver licenses. Read at the point of document inspection with commonly available scanners, IDMarc links together personal data and security features to ensure credential integrity and defend against falsified IDs from photo swapping and data alteration. IDMarc provides positive document authentication, age verification, cross-jurisdictional authentication, and forensic capabilities.

[1] *Consumer Fraud and Identity Theft Complaint Data*, January – December 2005, Federal Trade Commission, January 2006

[2] *Preventing Terrorist Attacks on U.S. Soil: The Case of the Wrong Package Falling into the Right Hands*, FBI Press Room, Headline Archives, 04/09/04

[3] *Traffic Safety Facts, Crash Stats*, NHTSA, August 2005

Under a 2004 grant from the NHTSA, Digimarc Corporation selected the Nebraska Department of Motor Vehicles (DMV) to take part in a pilot program – the ***"Operational Pilot of Digital Watermarking Reading for Driver License Authentication and Traffic Enforcement Support,"*** which was designed to provide, access, test, and validate new capabilities for authenticating driver licenses. The pilot included driver license inspection within retail, law enforcement, and DMV environments with the goal of enhancing traffic safety and driver license security through the use of digital watermarking in the State's driver licenses.

Five operational scenarios, or vignettes, were fielded:

- In-Car Inspection for Law Enforcement
- Office Inspection (DMV, Police, Commercial Vehicle Weigh Station)
- Point-of-Sale Inspection
- Mobile Inspection for Civilian Use
- Mobile Inspection for Law Enforcement

Digimarc installed systems and trained users on each of the five vignette configurations. The digital watermark scanners were installed in a total of 18 point-of-sale sites, 30 office sites, and 35 law enforcement sites, and were used in "real time" for an average of 30 days. Of the total of 83 scanning devices deployed, 45 were mobile or hand-held units, and 38 were desktop units attached to PCs. At the conclusion of the pilot, Digimarc staff interviewed the users regarding their experience with and response to the digital watermarking technology.

Nebraska Overview

In years past, prior to the rollout of the state's new digital driver license and enhanced issuance system, Nebraska—like many states—had to deal with a driver license that was easy to alter or duplicate. In fact, Police Officer Brian Ward joked about a training course he attended with a colleague from the Florida Division of Alcohol and Tobacco. The colleague commented, "*I never knew there were so many people from the state of Nebraska*," in reference to the large number of fake Nebraska driver licenses he confiscated in Florida bars during spring break.

Nebraska's goals for their new system were to bring the highest level of security and integrity to their state driver license and meet the governor's challenge of providing the most secure driver license in the country. "*The vision of the agency really is to focus on the customer, deliver a secure driver license, and provide the highest level of customer service possible*," said Beverly Neth, Director of the Nebraska Department of Motor Vehicles.

The development of Nebraska's current driver license issuance system included input from a broad group of stakeholders, including; law enforcement, retailers, the Liquor Control Commission, State Patrol, and advocacy groups such as Mothers Against Drunk Driving (MADD) and Project Extra Mile. To gain approval for the system from the legislature, the team cited numerous advantages such as machine-readable technology for law enforcement and the ability for retailers to reliably determine if an individual was over the age of 21, as required by Nebraska policy on underage drinking laws. The pilot provided a means to prove out these benefits.

When the pilot opportunity came along, Director Neth saw it as a chance to accomplish two primary goals:

1. Add another level of security to Nebraska's driver license that was cross-jurisdictional and would enhance public safety
2. Help retailers meet the State's goals of controlling the sale of age-sensitive products while balancing the privacy of the ID holder

"*Because of the type of information contained in the digital watermark, we saw this as truly a win/win situation,*" said Neth. "*The retailers wanted something they could point to that showed they went through a process to authenticate the card. Digital watermarking gives them that. We wanted something that was not going to provide a great deal of personal information to someone looking at or scanning the card.*"

With the Digimarc Digital Watermarking Technology Pilot Program, Nebraska became one of a growing number of states to implement IDMarc as part of its license issuance program. Today, more than 60 percent of the Nebraska licenses in circulation carry this digital security feature, and the Nebraska DMV has recently submitted a quote request to Digimarc to outfit 31 additional Nebraska DMV workstations with IDMarc. Nationwide, 16 other states are issuing or have committed to issue digital watermark secured identity documents, and 13 states have the feature currently in production.

IDMarc in Action

Portable IDMarc inspection devices were successfully deployed in patrol cars, with officers on foot, on the University campus, and at one truck weigh station. The liquor control portion included bars, nightclubs, restaurants, convenience, liquor and grocery stories, and one private enforcement service. Additionally, desktop scanners with IDMarc authentication technology were installed in municipal police department offices, in forensic laboratories, and in various offices of the Nebraska Department of Motor Vehicles.

In addition to in-car inspection of drivers and driver licenses, Nebraska police officers often patrol bars and nightclubs to check for heavily intoxicated people and underage drinkers. They also help to educate bar and package liquor store owners on how to spot a false ID. While visual inspection is somewhat effective for those already highly familiar with in-state driver licenses (such as police officers), it is less so for those less experienced or untrained in visually spotting fake IDs, or where visibility is limited, where staff are constantly distracted, or in validating out-of-state driver licenses not commonly seen by bar or retail sales staff.

In general, retailers of alcohol are desperate for methods that allow them to be certain they are selling only to customers who meet the legal criteria. One location where the pilot took place was Bill's Liquor Store in Kearney, NE. This liquor store had almost lost their license when it was discovered they had sold liquor to someone under the age of 21 who was later killed in a car crash. The driver license authentication pilot provided them with a means to rebuild their integrity and protect their license to do business.

As a part of the Digimarc Digital Watermarking Technology Pilot Program pilot, several bars and retail establishments were equipped with point-of-sale reader devices that allowed them to verify the information printed on a driver license—even an unfamiliar out-of-state driver license—against the information contained in the digital watermark. By doing so, they were able to determine if a driver license was valid or not and which, if any, age-controlled products the DL holder was old enough to purchase. The scanner/reader devices proved invaluable in instantly determining whether or not the license presented was authentic, as well as validating the age of the DL holder.

Several retailers reported that just the public's knowledge they were using digital watermark scanning devices deterred people from trying to use fake IDs. This same phenomenon was reported by a private security company that was hired to use the hand-held readers to authenticate driver licenses at the Nebraska State Fair; it created a visible deterrent and helped to curb the number of underage drinkers disrupting the event.

When surveyed at the conclusion of the pilot program, 100% of the retailers in the program reported that the digital watermarking feature gave them confidence that the ID was authentic. And the most common "objection" noted was that the digital watermarking feature needs to be *more* prevalent, especially in environments where large numbers of out-of-state licenses need to be authenticated.

Inspection Process

For law enforcement scanning a driver license "in the field," the IDMarc Inspector Series software displays an indication of validity, an image of the card, and complete digital watermark data. If the digital watermark rating is "Valid," officers are then able to submit a National Crime Information Center (NCIC) inquiry by document number with query results displayed in the viewer. If the digital watermark comes back as "Invalid" or absent the officer or other authorized user can open an image file to view examples of watermarked cards currently in production.

In an office environment, the IDMarc software displays all of the above—that is, an indication of validity, an image of the driver license, and complete digital watermark data—as well as a reminder to match the ID photo to the ID holder. In the case of an invalid card, the reason for failure is displayed along with forensic data. If no digital watermark is found, the system offers users information on cards that are or are not watermarked. The driver license image and digital watermark data are logged for later use in reporting.

In retail outlets a small card scanner is placed at the checkout stand to acquire an image of the front of the driver license. This image is then analyzed through the checkout monitor for the digital watermark security feature. In addition to determining the validity of the driver license, the user interface shows the age and birthday of the ID holder with symbols to illustrate which age-restricted products (cigarettes, alcohol, or lottery tickets) can be sold to the card presenter. If the ID holder is over 21, all three symbols are circled in green.

Results

Nebraska staff, operators, and officers all said the Digimarc IDMarc system exceeded all their expectations—and then some. "*Digimarc really came in and gave a great deal of respect to the Nebraska DMV staff. The listened to our suggestions, our comments, and our thoughts,*" said Director Neth. "*I think they put together a fantastic system that when rolled out, stayed up... and has stayed up ever since.*"

Overall, the responses of the test users to the digital watermark feature were positive, as shown in the following chart:

Survey Question	Yes	No
Do you believe that the feature is beneficial to you?	92%	8%
Does the feature give you confidence that the ID is authentic?	97%	3%
Would you use this in the future?	97%	3%
Would you purchase hardware that uses the Watermark feature? (retail only)	86%	14%

Of those point-of-sale retailers who used the system, 100% said that a valid read from the watermark gave them confidence that the DL was authentic. Those who said they would not purchase the hardware (18%) reported that "the technology is great" but that there are too many out-of-state driver licenses that are not digitally watermarked and cannot be scanned, which makes the devise less useful to them. When more driver licenses have digital watermarks, retailers state they would be more likely to invest in the authentication hardware.

Law enforcement officials also reported 100% confidence that a valid read from the watermark meant the DL was authentic. Police officers who used the in-car portable devise reported the system worked well and they liked the technology but using the scanners did not improve workflow because officers are experienced enough to visually authenticate most driver licenses. However, one respondent commented that they "like the idea of having a way to backup an officer's visual inspection." One area where the IDMarc proved especially effective in the officers' eyes was in authenticating out-of-state licenses which they might not be familiar with; one officer stated he was able to authenticate the digital watermark on an out-of-state license from Minnesota.

The group of participants who used IDMarc scanners in an office setting also felt positive about the feature. Fully 100% of those surveyed reported that they believed the device was beneficial, that it gave them confidence that the scanned ID was authentic, and that they would use it in the future. The most common issue reported was a desire for better integration with other systems such as bar code readers.

About Digimarc

The evolving role of the driver license in the US market—from evidence of competency to a means of personal identification to a secure credential—the events of 9/11, and the rapid advent of the Internet information age have stimulated a demand for a level of security in today's state-issued driver license which will allow it to be used with confidence as the de facto standard for establishing citizen identity in the United States, as well as an obstacle to identify theft.

Digimarc remains dedicated and focused on delivering high-quality, secure driver license issuance solutions that provide citizen access to a growing number of services and privileges, such as: applying for a passport, authorization to operate a motor vehicle, boarding an airplane, or purchasing age-restricted products.

Digimarc secure driver license solutions enable states to deter counterfeiting, enhance traffic safety and national security, combat identity theft and fraud, and facilitate the effectiveness of voter ID programs. The company has partnered with state customers through every major transition in driver license systems—and has issued billions of credentials worldwide, including two-thirds of the states' driver licenses, and identification solutions for more than twenty countries. Digimarc is the *only* company in the world focused on meeting the unique and growing needs of today's driver license issuers.

IDMarc digital watermarking is rapidly being adopted by many jurisdictions in the US responsible for driver license issuance as the standard for cost-effective, multi-purpose reading devices that enable reliable, cross-jurisdictional authentication of driver licenses and IDs that are secured with digital watermarks. Reading applications span law enforcement, retail sale of age-controlled products, banking, and border crossing. Digital watermarking technology has been proven over the past decade in a variety of commercial products, and has been applied to various authentication and high security applications worldwide.

Testimony of Michael P. Everitt
Unit Chief Forensic Document Laboratory
Office of Investigations
U.S. Immigration and Customs Enforcement
Department of Homeland Security
Before
The Senate Committee on Finance
Regarding
Fraudulent Documents
August 2, 2006
Washington, DC

Good morning Chairman Grassley, Ranking Member Baucus, distinguished Members of the Committee; I am pleased to be here today to discuss the technical aspects of fraudulent documents. The U.S. Immigration and Customs Enforcement (ICE) Forensic Document Laboratory (FDL) is the premier forensic document laboratory in the world and is a forensic crime laboratory dedicated exclusively to fraudulent document detection and deterrence. The FDL is accredited by the American Society of Crime Laboratory Directors—Laboratory Accreditation Board (ASCLD/LAB) in questioned documents and latent prints. The FDL's mission is to detect and deter domestic and international travel and identity document fraud by providing a wide variety of forensic and support services to all Department of Homeland Security (DHS) components, including ICE, U.S. Customs and Border Protection (CBP), U.S. Citizenship and Immigration Services (USCIS), the United States Secret Service (USSS), and the United States Coast Guard (USCG). The FDL also supports other federal, state, and local agencies, as well as foreign government law enforcement and border control entities. The FDL is one part of a comprehensive solution that is necessary because fraudulent documents are used by illegal immigrants who are living and working throughout the nation, in every state and in many different industries. With this in mind, the Administration supports comprehensive immigration reform that increases border security, establishes a robust interior enforcement program, creates a temporary worker program, and addresses the problem of the estimated 11 to 12 million illegal immigrants already in the country.

The FDL consists of two sections: Forensics and Operations. The Forensics Section is responsible for conducting all forensic work on documents and related material submitted to the FDL for forensic examination. The Operations Section provides training and real-time support, produces the publications distributed by the FDL, and provides analysis of the information gathered from documents submitted to the laboratory for forensic examination. The Operations Section takes information developed by the Forensics Section and ensures that it is distributed to the field via training, real-time support, and publications.

The Forensics Section is staffed with Forensic Document Examiners, Fingerprint Specialists, and Forensic Photographers. We are currently in the process of recruiting personnel to staff a new ink chemistry unit, which will add an additional dimension to our forensic services. Prior to conducting examinations, forensic document examiners must successfully complete an in-house 30-month training program (24 months of training followed by a six month apprenticeship) that includes instruction on all facets of document examination, printing processes, security features, wet and dry seals, typewriter examinations, and handwriting analysis. This comprehensive training is necessary to acquire and maintain laboratory accreditation and personnel certification. The FDL-provided training is in addition to the requirement for a Bachelor's degree (many of the FDL Forensic Document Examiners have Master's Degrees in Forensic Science and are working on independent board certifications). The primary responsibility of the Examiners is to conduct examinations of fraudulent documents submitted to the FDL. These documents are typically seized from individuals attempting to enter or remain in the United States illegally, or from fraudulent document production operations.

FDL Fingerprint Examiners are experts in their field and routinely testify as expert witnesses in criminal and administrative proceedings arising from ICE and other agency investigations. The fingerprint unit uses the latest techniques and technologies to lift latent fingerprints from documents, document production equipment, wrappings, weapons, and other recovered material submitted to the laboratory. Using various Automated Fingerprint Identification Systems (AFIS), examiners attempt to identify individuals relevant to the investigation and then link these individuals to evidence in the case. The fingerprint unit also has a team of forensic photographers who assist all FDL staff with expert photographic services. These include capturing images of documents and other evidence under various forms of light, providing photographs and graphics for reports, and preparing court exhibits.

The FDL Operations Section is staffed by intelligence officers, many of whom have worked in large ports of entry and have extensive experience with travelers and the documents they use. The Operations Section provides real-time support to the field, produces a variety of publications, and provides fraudulent document recognition training around the world.

Real-time support is provided 24 hours a day, 365 days a year to assist all federal, state, and local law enforcement officers with questioned documents. This is accomplished by the FDL being manned from 6:00 am until 8:30 pm on weekdays, and manned after-hours and on weekends by on-call personnel who have secure access to FDL systems and databases and can provide this support remotely. Real-time support is also provided to non-law enforcement personnel that may have questions concerning travel and identity documents. These non-law enforcement entities include Department of State Consular Offices that adjudicate visa requests, and USCIS personnel who adjudicate benefit requests.

Document Alerts, Intelligence Briefs, and Reference Guides are produced, printed, and distributed to more than 800 law enforcement and border control agencies worldwide to assist officers in identifying fraudulent documents in circulation. Many of these publications are also posted on various DHS Internet portals to make them available to as many agencies as possible. All of these publications are high quality products with descriptive text and detailed graphics. The publications are designed to convey the information in a clear and concise manner, which allows the front line officer to absorb the information quickly and retain that information for use in the field.

The Operations Section also designs and provides training programs on fraudulent document recognition. FDL Operations Section personnel routinely conduct fraud detection training for DHS personnel and other federal, state, local and foreign law enforcement officers. This year alone, the FDL has trained more than 2,200 people in locations all over the world, including the United States, Pakistan, Botswana, Qatar, UAE, Bangladesh, Bahrain, Senegal, Belize, El Salvador, and the Bahamas. Of the individuals trained this year, nearly 450 were from CBP. We also receive requests for training from state and local law enforcement agencies and from private concerns. The FDL has responded to these requests, though the amount of training that can be completed is limited by our available resources. To meet the increasing demand for these services, the FDL created "Train-the-Trainer" classes. These classes allow us to train persons in other agencies who then conduct fraudulent document recognition training with FDL support. The program allows us to expand the number of fraudulent document recognition training classes conducted each year.

The Operations Section also includes an analysis group. This group gathers intelligence from documents sent to the laboratory, whether they were submitted for forensic examination or for analysis and safekeeping. The intelligence from these documents is collected, analyzed, and then distributed to the field as investigative leads, or is used to produce Document Alerts and Intelligence Briefs.

Because the Forensics Section and the Operations Section are co-located at the FDL, we can attack the problem of fraudulent documents in a coordinated manner and provide the necessary services to the field from a central and highly specialized facility.

Occasionally there are misconceptions about what constitutes a fraudulent document. Many people think that fraudulent documents are counterfeit documents. While counterfeit documents are in fact fraudulent documents, the latter also include altered and fraudulently obtained documents. Altered documents include those with erasures, substituted photos, and thin-layer laminate overlays. In most cases, altered documents are actually genuine documents that have been altered for fraudulent use. Fraudulently obtained documents are genuine documents that have been obtained by fraudulent means. These means could include the use of counterfeit "breeder documents" to obtain a genuine document, or the theft or purchase of a genuine document, which is later altered, from the true owner. Stolen blank documents also pose a problem. Over the years, the FDL has seen many stolen blank passports, which are personalized to create a fraudulent document. These documents are particularly hard to detect because they are genuine blanks.

Some criminals use a genuinely issued identity document in a fraudulent manner. There are many ways to do this. The most common method is impersonation, in which one person uses the genuine identity document of another person with similar physical features. Impostors are frequently intercepted at ports of entry along our border with Mexico, after attempting to use stolen or purchased Resident Alien or border crossing cards to enter the United States.

Fraudulent documents are also meant to mislead. "Fantasy documents" mimic genuine forms of identification in appearance without actually purporting to be legitimate government-issued forms of identification. Examples of fantasy documents include "Klingon" passports and "International" drivers' licenses (not to be confused with the International Driver's Permit, which is a translation of a driver's license for international use issued by automobile associations). While these examples are extreme, official fantasy documents that purport to be from a newly established country would deceive many people. They take advantage of the thousands of authorities that issue genuine identification documents domestically and abroad. Individuals obtain these items via the Internet as novelties and then present them as valid forms of identification. At present, there are no laws that make the importation of fantasy documents into the United States illegal and therefore subject to seizure.

Document producers and those who issue legitimate documents are in a constant battle to develop new production methods and security features to make the identification documents they issue more secure. DHS has revised and updated many of the documents associated with the immigration process. The U.S. Department of State has recently introduced a new version of the U.S. passport that includes an integrated electronic chip as well as other security features intended to thwart those who would counterfeit or alter the document.

Technological advances, which have made commercial quality scanning and printing widely available, have significantly increased the quality of fraudulent documents. The purveyors of fraudulent documents make full use of commercially available scanning and printing technology to manufacture better fraudulent documents, including not only hardware, but also high quality graphic software that includes advanced techniques such as layering. Digital printing technology has been used in the majority of the fraudulent documents examined by the FDL. Sophisticated computers, software, digital scanners, and color inkjet or laser printing equipment are now routinely recovered when fraudulent document operations are discovered in the United States and overseas. For example, many of the altered passports and identity documents encountered by U.S. forces in Iraq incorporated digitally printed components. As high quality scanning and printing equipment becomes less expensive and more readily available, digitally produced fraudulent documents become more difficult to detect. This problem is further complicated by the increased use of digital printing technologies to create genuine identification documents. Genuine document-issuing authorities often select digital printing technologies to create or personalize genuine documents because they are less expensive than traditional methods such as offset or intaglio printing and because the lower costs allow the process to be deployed to the field, rather than necessitating reliance on production centers. The result is that digitally printed fraudulent documents can be more difficult to detect by officials responsible for examining documents, such as ICE special agents, Border Patrol agents in the field, CBP officers at ports of entry, or airline security personnel overseas.

Detection of high quality fraudulent documents requires an increased level of training for front-line staff to significantly enhance their expertise. Ten years ago, border inspectors could look for some simple points of detection to identify fraudulent identity documents; however, training sessions today are often crash courses in forensic document analysis. The marriage of digital technology and traditional printing methods can create fraudulent documents that are very difficult to detect. Security features are specially designed to thwart reproduction by scanners or other digital equipment. Optically Variable Devices (OVD) such as holograms and kinegrams, specialized inks, and various forms of security printing techniques cannot be duplicated easily by commercially available computer equipment, so these features are often used to make documents more secure. However, the producers of fraudulent documents are becoming better at mimicking these features or circumventing them altogether.

There are many reasons for the proliferation of fraudulent documents. ICE typically sees false documents being used by illegal aliens who live and work in the United States. However, foreign nationals who seek to enter the United States and cause harm to our Nation represent another market for fraudulent documents. The quality of fraudulent documents used for international travel must be better than domestic fraudulent documents because they will be shown to people who routinely examine travel and identity documents. CBP officers inspect the documents of passengers arriving by air or sea, as well as those attempting to enter over land. Last fiscal year, CBP inspected more than 430 million people coming to the United States. In many cases, illegal migrants, criminals and even terrorists have tried to blend in with returning citizens, legal residents and lawful visitors by using fraudulent documents.

Fraudulent documents are used in different ways for different reasons. Domestically, there is an enormous market among illegal immigrants to demonstrate work eligibility. Current laws require employers in the United States to verify that their employees are eligible to work legally in this country. To do that, employers complete the I-9 Employment Eligibility Verification form, which has a list of acceptable documents to demonstrate identity and employment eligibility. Unfortunately, the vast majority of the people responsible for reviewing documents presented for employment have never received any type of training in fraudulent document recognition. Also, under current law, employers do not have an obligation to verify the validity of the document, but are only required to certify that the document appears to be genuine and relates to the individual in question.

The FDL has produced the *"Guide to Selected U.S. Travel and Identity Documents,"* Form M-396, which is publicly available. The latest version, published in late 2005, is a high quality color booklet with information and photographs (front and back) of the most common U.S. travel and identity documents. These documents include the U.S. Passport, U.S. Naturalization Certificate, Resident Alien Card, the Permanent Resident Card, the Employment Authorization Card, Reentry Permit, Travel Document, U.S. Visas, Border Crossing Card, and Social Security Card. This reference guide, which is one of many published by the FDL, is helpful to employers who are responsible for completing I-9 forms. The FDL uses every opportunity to distribute this publication to employers, law enforcement, and others who may come in contact with these types of identity and travel documents and we continue to explore additional methods to increase distribution.

Genuine travel documents, like passports, visas and residence cards, contain many security features meant to deter the creation of fraudulent documents. As identity documents have become more secure, the number of "look-alike" impostors trying to get through the U.S. border has increased dramatically.

This does not mean, however, that the number of fraudulent documents has diminished. Individuals with fraudulent documents continue to be intercepted at the border and in the interior. A common alteration to travel and identity documents with holograms and other visual security devices involves simply covering the original photograph and personal data with the photo and information of the person who wants to use the fraudulent document. This is accomplished by using a computer to print the bearer's information onto a clear piece of plastic, known as a thin layer laminate, laying it over the original document, and holding it in place with adhesive. This technique preserves the appearance of the documents and most of the holograms. The original photograph and information are eradicated to prevent a double-image from appearing and the laminate conceals the eradications making it more difficult for examining officers to detect.

At the FDL, we have seen some very sophisticated uses of thin layer laminates to alter documents. In one case in particular, we saw the use of a thin layer laminate by an imposter. A male imposter from Asia attempted to use a U.S. passport issued to a U.S. citizen of Asian descent. The imposter's facial image had been printed in color on the reverse of a thin layer laminate. Using adhesive, this laminate had been placed over the biographical page of the U.S. passport to change the appearance of the passport's original photograph, which was still in place, to that of the imposter. This sophisticated attempt was detected by an alert CBP officer who noticed the imperfect edge of the thin layer laminate.

Some counterfeiters are highly sophisticated and have been able to produce highly deceptive versions of U.S. visas, or even entire passports, by effectively simulating the security features found in genuine documents. Forgers in Brazil and Colombia have steadily improved counterfeit versions of the U.S. visa. Analyses of documents submitted to the FDL over the last several years have shown that many documents intercepted at various ports of entry have common identifying features, and in each successive generation the forgers continue to show improvements, making their documents more difficult to identify and the people traveling with them more difficult to detect.

Counterfeiters in Southeast Asia have created high-quality passports or passport pages for passports from Visa Waiver Program countries, which permit entry to the United States without first obtaining a visa. Again, FDL analysis has revealed a continuing improvement in these counterfeits over time as the manufacturers learn how to improve their products and make them more deceptive.

Just as with any other illegal activity, the government must continue to deter, detect and act against those who use and facilitate the use of fraudulent documents. Within the Department of Homeland Security, ICE has the most expansive investigative authority and the largest force of criminal investigators. Our broad mission is to protect the American public by combating the terrorists and criminals who seek to enter our country illegally and pose a risk to our national security. Among our investigative priorities, ICE is leading the effort to identify, disrupt and deter those organizations that engage in the fraudulent document trade, as well as organizations that facilitate the fraudulent filing of immigration benefits with USCIS. Within ICE, the Identity and Benefit Fraud Unit has programmatic oversight over investigations of immigration fraud in all its forms.

Immigration fraud generally falls into two categories: benefit fraud and identity fraud. Benefit fraud, or the willful misrepresentation/omission of a material fact on a petition or application to gain an immigration benefit, is a particularly serious and a highly lucrative form of organized white-collar crime. Immigration benefits confer lawful status upon an individual and as such, their value to illegal aliens, terrorists, and criminals is immense. Identity fraud involves the manufacturing, counterfeiting, alteration, sale, and/or use of identity documents and other fraudulent documents for criminal activity, including the circumvention of immigration laws. More often than not, the use of fraudulent documents and the counterfeiting of government forms is an integral part of filing these fraudulent applications. I would like to take a few minutes to highlight some of the initiatives of the Identity and Benefit Fraud Unit, as well as some of our recent successful investigations.

In September 2003, ICE and USCIS initiated a joint anti-fraud initiative by establishing Benefit Fraud Units and Fraud Detection Units, respectively. By working together, our agencies have identified thousands of fraud leads and developed new and more efficient ways to address those aliens who receive immigration benefits through fraud. This is an evolving relationship and we are very excited about the progress our agencies have made to address immigration benefit fraud.

Additionally, as part of the Department's Secure Border Initiative, ICE established the Document and Benefit Fraud Task Forces to eliminate vulnerabilities within the immigration process. These task forces focus efforts to combat immigration fraud through aggressive and comprehensive investigations and prosecutions by leveraging the resources of other DHS components, the Offices of the U.S. Attorneys, and other federal, state and local law enforcement agencies. The task forces use a variety of law enforcement tools and authorities to achieve criminal prosecutions and financial seizures.

In April 2006, ICE formally announced Document and Benefit Fraud Task Forces in 11 locations, including Atlanta, Boston, Dallas, Denver, Detroit, Los Angeles, New York, Newark, Philadelphia, Saint Paul, and Washington, DC. These task forces formalize and strengthen pre-existing working relationships ICE had with our partner agencies. These task forces have already achieved significant success. Based upon the support we have received, ICE is evaluating the expansion of these task forces to additional locations.

By working with the Identity and Benefit Fraud Unit and these task forces, the FDL is one of the critical investigative tools utilized by ICE in the fight against immigration fraud and counterfeiting. The FDL and the Identity and Benefit Fraud Unit are ensuring that as our task forces expand in scope, the agents and officers assigned to these investigations have access to every resource that ICE and the Department have to offer.

Recently, ICE announced several significant immigration fraud investigations that are due in large part to the work of the Identity and Benefit Fraud Unit, the FDL and our task force partner agencies.

One of our greatest and most recent successes was the dismantling of the Castorena Family Organization (CFO). This group was a large-scale criminal organization with more than 100 key members who oversaw cells of 10 to 20 individuals in cities across the United States. The organization was involved in the manufacture and distribution of high-quality counterfeit identity documents, including social security cards, birth certificates, marriage certificates, U.S. and Mexican driver's licenses, resident alien cards, work authorization documents, proof of vehicle insurance cards, temporary vehicle registration documents, utility bills, and a host of other documents.

Our investigation, conducted in conjunction with the IRS, Social Security Administration Office of the Inspector General, and the U.S. Postal Inspection Service, revealed that the CFO began in Los Angeles in the late 1980s, manufacturing and selling counterfeit alien registration and Social Security Cards. The organization expanded its counterfeit document operations to cities across the United States, including New York, Chicago, Las Vegas, Denver, Atlanta, Albuquerque, and others. ICE investigations targeted cells of this organization in Los Angeles, New York, Chicago, Atlanta, Miami, Dallas, San Antonio, Las Vegas, Albuquerque, Denver, Lincoln, NE, and Des Moines, IA.

In Denver, the Castorena investigations resulted in the criminal prosecution of more than 50 individuals. Dozens of additional members of the CFO in Denver have been arrested and deported to Mexico, Colombia, and El Salvador. ICE and task force agents in Denver seized more than 20 computerized laboratories affiliated with the CFO that were used to manufacture high-quality counterfeit identity documents. As part of this investigation, ICE also seized computers and silkscreen printing templates used to produce counterfeit documents, as well as handguns.

Our investigation revealed that CFO cells in various U.S. cities were exceptionally well organized. Cell leaders typically kept schedules with the names of each counterfeit document vendor and the times they reported to a designated area to sell fake documents. The local cell leaders also recorded the number and type of false documents sold by vendors during their "shifts," as well as the funds collected for each transaction.

These vendors were allowed to keep a portion of the proceeds, with the remainder passed to the local cell leader. Cell leaders, in turn, passed on a portion of the proceeds to the senior leaders of the CFO, who in turn charged a "rent" or "franchise" fee of as much as $15,000 per month for cell leaders to operate in a particular U.S. city. These funds and other proceeds of counterfeit document sales were funneled to Mexico and other locations for those overseeing the CFO. This enterprise was a big business and the American Express Corporation attributed more than $2 million in losses to counterfeit identification documents that were traced to the CFO in Los Angeles alone.

On June 17, 2006, Mexican law enforcement officers and ICE Attaché Mexico City agents arrested Pedro Castorena-Ibarra, a citizen of Mexico, and head of the CFO, pursuant to a provisional arrest warrant in Guadalajara, Jalisco, Mexico. Castorena was the top priority on ICE's Most Wanted fugitive list. ICE is assisting the U.S. Attorney's Office, which is currently pursuing extradition.

The FDL performed forensic document examinations on numerous questionable, high-quality documents manufactured by the CFO. The FDL identified numerous latent fingerprints on individual items of evidence and counterfeit identity documents as belonging to members of the CFO, which then were used during their prosecution. Additionally, the FDL identified several fingerprints that were imbedded in the computer templates utilized by members of the CFO to manufacture individual counterfeit identity documents throughout the United States. Through our analysis of evidence from this investigation, the FDL was able to definitively match seized counterfeit identity documents manufactured by members of the CFO to more than 400 investigations and seizures in more than 50 different cities across 33 states.

Our Boston Document and Benefit Fraud Task Force, consisting of agents from ICE, the Social Security Administration, the USSS, the Department of State, and the Middlesex County Sheriff's Office, is engaged in multiple document fraud investigations. Between June 5 and June 8, 2006, ICE agents assigned to the Document and Benefit Fraud Task Force executed nine federal arrest warrants, four search warrants, and one consent search in furtherance of these ICE-led investigations. The search warrants resulted in the seizure of six computers and document-making implements at five residences.

The FDL is supporting these task force cases by conducting analysis of latent fingerprints found on counterfeit green cards seized during the investigation. The FDL is also examining counterfeit documents purchased from different vendors to determine if the documents were produced by the same manufacturer.

In Operation Mandalapa, a product of the joint anti-fraud initiative undertaken by ICE and USCIS, our Newark, New Jersey Document and Benefit Fraud Task Force initiated a large benefit fraud investigation based upon referral from the Benefit Fraud Unit in Vermont and USCIS. Agents identified more than 1,000 labor-based petitions for skilled computer workers filed on behalf of Indian and Pakistani nationals. Numerous companies were identified in the petitions and were determined to be shell companies created for the sole purpose of filing fraudulent petitions on behalf of foreign workers. On January 10, 2006, ICE and Department of Labor agents executed seizure warrants relating to four bank accounts totaling more than $2.4 million and two brokerage accounts amounting to nearly $3.3 million. Agents also seized two luxury vehicles with a combined value of approximately $100,000. On June 19, 2006, based on the strength of the evidence against him, the defendant who set up these companies pled guilty and stipulated to the forfeiture of the $5.7 million and the two vehicles.

In the Mandalapa case, the FDL conclusively determined that the approval stamps used on labor certifications were, in fact, color copies and not original stamps. The FDL provided latent fingerprint examination and handwriting analysis on key documents that would have potentially been used as evidence had the case gone to trial.

Fraudulent travel and identity documents are a worldwide problem, which will continue to challenge law enforcement officials in the United States and abroad. As long as identification is required to travel and obtain goods or services, criminals will attempt to produce fraudulent documents. Recently, there has been an emphasis on deploying systems to validate documents. While the FDL supports these programs, we believe these systems cannot take priority over the continued development of stronger travel and identification documents. Electronic validation systems will not always be available to the officers, employers, or others who may need to verify document authenticity. To that end, the FDL provides Counterfeit Deterrence Study teams, consisting of a Forensic Document Examiner and an Intelligence Officer, to work with entities designing new travel and identity documents to ensure that they incorporate security features that truly make them resistant to fraud. The development and distribution of quality documents will be expensive as it will require replacing old document production systems and infrastructure; however, the investment will pay healthy dividends in security.

On behalf of the men and women of ICE and specifically the men and women of the Forensic Document Laboratory, I thank the Finance Committee and its distinguished members for your continued support of our work.

I would be pleased to answer your questions.

U.S. Senate Committee on Finance

"Border Insecurity, Take Two: Fake ID's Foil the First Line of Defense"

August 2, 2006

Testimony of Janice L. Kephart

Introduction

Thank you for the opportunity to submit testimony for the record on *terrorist travel, the U.S. border inspection process* and the *Western Hemisphere Travel Initiative* (WHTI). My testimony is based on the following work, plus additional research specific to today's hearing:

- As a counsel to the Senate Judiciary Subcommittee on Technology, Terrorism and Government Information prior to 9/11;
- As a counsel on the 9/11 Commission "border security team" which produced the *9/11 Final Report* draft recommendations and analysis;
- As an author of the 9/11 staff report, *9/11 and Terrorist Travel*;
- As the senior consultant for a privately funded and unreleased report entitled "An In-Depth Analysis of the Structure of Al Qaeda and Militant Islamic Terrorist Groups in the United States: The Enterprise of Terror in the United States" in March 2005; and
- As the author of a September 2005 Center for Immigration Study report, "Immigration and Terrorism: Moving Beyond the 9/11 Staff Report on Terrorist Travel."

At the Commission, I was responsible for the investigation and analysis of the INS and current DHS border functions as pertaining to counterterrorism, including the 9/11 hijackers' entry and acquisition of identifications in the United States. My team also produced the drafts of the *9/11 Final Report* recommendations that were unanimously agreed to and refined by 9/11 Commissioners led by Governor Tom Kean and Representative Lee Hamilton.

I want to thank both Chairman Grassley and Ranking Member Baucus for holding this important hearing on the GAO's findings pertaining to the need to tighten border inspection policy and processes. I am glad the Committee remains supportive of the policy we put forth in the *9/11 Final Report* of securing our borders alongside assuring facilitation for low risk commerce and commuters.

It is my hope that this Committee will continue to exercise their oversight authority on the important issue of terrorist travel and overall border security. I hope your Committee will help insure that any immigration bill sent to the President contains strong language pertaining to tightening border inspection, including the timely implementation of WHTI. WHTI was recommended by the 9/11 Commission to both tighten border security and streamline the inspection process, especially at our land ports of entry. We must continue oversight hearings that highlight how essential border security is to national security, and set out agendas for achieving effective and efficient border security. We cannot afford to permit different aspects of our borders—such as the inspection process- to be bifurcated from the discussion of national security. Our economic strength as a nation is only as strong as our national security. We must continue to work alongside our friends in the trade and tourism industries to achieve both security and facilitation.

Assuring our border inspection process is fast, fair and complete is essential. It is also doable. We simply need to prioritize how personnel, budgets and technologies are allotted and deployed with precision. The focus must be on how to properly train and equip our border inspectors so that procedures assure security of our borders in the most effective and least intrusive manner possible. It cannot wait. It has been nearly five years since 9/11 and our border inspection is still waiting for the significant upgrades in procedures and processes that should have been forthcoming after 9/11. And while WHTI changes policy to shore up significant, large and sweeping holes in our border security so that *all persons* seeking entry into the United States show standardized travel documents or equivalents that can be vetted, this policy will not reach its potential in implementation unless DHS does its job and partners with the private sector to match policy with solutions that are tried and workable in the border inspection environment.

If we fail to upgrade our border inspection regime now, or permit WHTI to be defeated either by law or poor follow-through by DHS in the coming months, the result will be that terrorists, drug dealers and those who abuse our lax security will continue to easily move through our border system with fake documents or no documents at all. The policy in effect today at our ports of entry, the Western Hemisphere Travel Exception, actually encourages fraudulent entry by permitting any traveler claiming to be a U.S. citizen to talk their way into the United States or show any variety of identity document and claim to be from the Western Hemisphere.[1] And at least on the Canadian border, surveys show that 40% of Canadians state they have not been asked to show any identification when seeking entry into the United States. In testimony today before this Committee, GAO today again proves the point when in 42 of 45 instances between 2003 and 2006 GAO agents with counterfeit documents were able to flash false papers, or in a few instances, no papers at all, and enter the United States. Consider that number transferred over to attempted terrorist entries, and we have much to be concerned about.

The only way to secure our borders is to make the terrorists choose between using a passport, applying to a trusted traveler program, or enter illegally. As long as a terrorist can pose as a U.S. citizen or traveler from the Western Hemisphere by producing a birth certificate, fake driver license that can't be verified, or other forms of identification that

[1] Take for example Venezuela, only within the last few months singled out by the State Department for close U.S. border examination of Venezuelan travel documents nearly three years after information surfaced that President Chavez had initiated a policy to assure that terrorists passed anonymously through their border system. Only a short distance from the Caribbean, (and adjacent to the island of Trinidad known for harboring at least three major terrorist organizations), terrorists passing through Venezuela for safe harbor need only have moved into the Caribbean, attain a counterfeit U.S. driver license or birth certificate, and easily make their way into the United States.

can be neither verified for identity, checked against a watchlist, or authenticated as a legitimate document, the Western Hemisphere Travel Exception is an open invitation to enter and embed in the United States with little disincentive not to try.

We can argue all we want about how to achieve the balance between actual secure borders and facilitation of trade and commerce, but we cannot *ever* afford to say it is not important or there is a segment of our border apparatus to which security does not apply. Nor can we afford to unravel well-based recommendations of the 9/11 Commission and passed into law by this body. Lest we forget that September 11 has taught us that secure borders are a matter of national security, and to secure them we must remember that terrorists will use any means to enter and embed into the United States.

We must treat our borders as they truly are: as a marker of U.S. sovereign rights to assure that people who seek to come here are who they say they are, and will not cause a public safety or terrorist threat to American citizens. At the border, the passport is the manner in which we as a nation can better assure that the people who seek to come here do so for legitimate reasons. A top priority in all we do in border security must then be to assure practical, on the ground, security measures at our ports of entry and physical borders.

However, let me be clear: we need not give up privacy nor give up commerce to attain border security. In fact, with efficient and streamlined security, privacy and commerce are both enhanced. People and goods that should make it through the system in an efficient manner are more likely to be when the acceptable forms of travel documents go from dozens to one, and varieties of those forms go from thousands to one, and trusted or registered traveler/commercial programs augment the system as an alternate to a federally issued travel document.

In extensive testimony before the House Judiciary Subcommittee on Immigration, Border Security and Claims in June, I provided details of the threat of terrorist entry from the Western Hemisphere-- Canada, the Caribbean and Mexico. I will not repeat the litany of threats posed to the United States from terrorist entry in the Western Hemisphere here other than a few anecdotes of why it is not just the 9/11 hijackers we must look to in developing U.S. border security policy.

Findings regarding Terrorist Travel

The majority of the factual findings that support a more robust border inspection and WHTI are not found in *9/11 Final Report*, other than the supporting commentary in the recommendations section of that report. Instead, as the border team staff hired to support the Commission's work, we intended for our staff report, *9/11 and Terrorist Travel,* initially published on the web and then published in more complete book form by Hillsboro Press, to be the factual support for all Commission recommendations pertaining to stronger border inspection, including what became WHTI. Instead of rehashing the entire report here, what I wish to emphasize is that our recommendations were based not only on what we learned about terrorist entry and embedding tactics by the 9/11 hijackers, but also what we gleaned from thorough review of other convicted terrorists whose immigration stories remained relevant. The stories of 1993 convicted terrorists Ramzi Yousef, the Blind Sheikh, and Millennium bomber Ahmed Ressam, to name a few, are all relevant and their histories are told in detail in our report.

In addition, in independent studies I conducted after the conclusion of the Commission on current terrorist activity in the United States and another on terrorist abuse of the immigration benefits system, I found many more examples of terrorist abuse of our lax border inspection practices. What was, and continues to be, of even greater concern is how much terrorist entry we will never know about due to clandestine entry either over our physical borders or by bypassing our border inspection process at land ports of entry through presentation of fake documents or through no check at all.

Examples of terrorist entry over land ports of entry are anecdotal because we have no way to measure the extent of the problem, although we know terrorist cases involving significant cross-border terrorist traffic exist. Less well known examples include the bust of likely al Qaeda member Nabil Al-Marabh in the back of truck cab in the summer of 2001; the Hizballah cigarette smuggling case that operated between North Carolina and Canada in the late 1990s; and the recent bust of the terrorist cell in Ontario where two Georgia men arrested on terrorist charges here had visited the cell in Canada by bus. With few checks and little database entry by inspectors at our land ports of entry, we will never know about most cross-border terrorist traffic—let alone stop it- unless we shore up our border inspection personnel and processes.

Key Excerpts from *9/11 and Terrorist Travel*

Below is the index for our 275-page staff report *9/11 and Terrorist Travel.* I include it to remind the Committee that when our team made recommendations to the Commission to be included in the *9/11 Final Report*, we did so after careful deliberation. I will also remind the Committee that each staff team was comprised of Republicans, Democrats, and in our case, an Independent as well. We submitted nothing to the Commissioners for consideration to which our team did not agree unanimously.

9/11 and Terrorist Travel
Staff Report, August 21, 2004

The recommendation on requiring passports or a biometric equivalent for all persons seeking entry into the United States we all agreed on, in concert with then DHS Secretary Tom Ridge, our Executive Director Phil Zelikow, and with unanimous support from within our team and our Commissioners.

The following are key bits lifted from *9/11 and Terrorist Travel* for the purpose of setting out some of the key findings that the 9/11 Commission considered substantial support for its recommendation that Congress later termed the Western Hemisphere Travel Initiative.

1. Introduction: Factual Overview of the September 11 Border Story[2]

Terrorists travel for many reasons, including training, communicate with other terrorists, collect funds, escape capture and interrogation, engage in surveillance of potential targets, and commit terrorist attacks.

To avoid detection of their activities and objectives while engaging in travel that necessitates using a passport, terrorists devote extensive resources to acquiring and manipulating passports, entry and exit stamps, and visas. The al Qaeda terrorist organization was no exception. High-level members of al Qaeda were expert document forgers who taught other terrorists, including Mohamed Atta, the 9/11 ringleader, their tradecraft.

[2] See *9/11 and Terrorist Travel: A Staff Report of the National Commission on Terrorist Attacks Upon the United States* (Franklin, Tenn.: Hillsboro Press, 2004) at p. 3. It is available in book form at http://providence-publishing.com/Merchant2/merchant.mvc?Screen=PROD&Store_Code=PP&Product_Code=9ATT&Category_Code=FTANR

The entry of the hijackers into the United States therefore represented the culmination of years of practice and experience in penetrating international borders.

Acquisition of New Passports[3] Thirteen of the hijackers presented passports less than three weeks old when they applied for their visas, but the new passports caused no heightened scrutiny of their visa applications.

Ports of entry[4]
Once the operation was under way, the conspirators attempted to enter the United States 34 times over 21 months, through nine airports. They succeeded all but once. Border inspectors at U.S. airports were unaware of the potential significance of indicators of possible terrorist affiliation in conspirators' passports and had no information about fraudulent travel stamps possibly associated with al Qaeda. No inspectors or agents were trained in terrorist travel intelligence and document practices. The culture at the airports was one of travel facilitation and lax enforcement, with the exception of programs to interdict drug couriers and known criminals.

When they began to arrive at the U.S. airports in January 2000, the pilots traveled alone. With the exception of two of the hijackers, the "muscle" operatives arrived between late April and late June 2001. They came in groups of two or three, and in four cases were screened by the same inspector.

All but one of the hijackers presented visitor visas that immigration inspectors used to decide whether to admit them as tourists or on business. All but two of the nonpilots were admitted as tourists and were granted automatic six-month stays. This allowed them to maintain a legal immigration status through the end of the operation. One of the two nonpilots admitted on business was granted a one-month stay; he, along with another of the nonpilot operatives, was in violation of immigration law for months before the attack. The one pilot who came in on a student visa never showed up for school, thereby violating the terms of his U.S. visa. Another of the pilots came in on a tourist visa yet began flight school immediately, also violating the terms of his U.S. visa. This pilot came in a total of seven times on a tourist visa while in school. In both cases, the pilots violated the law after their entry into the United States.

Five hijackers attempting entry were referred by primary inspectors for a more intensive review by secondary inspectors. One pilot was referred at two entries, in one case by a customs inspector trained to look for drug couriers, and in the other by an immigration inspector thinking the pilot might be an intending immigrant. One pilot was referred for having the wrong visa and one nonpilot hijacker for failing to have a visa. Two others were referred for failing to complete their arrival and customs forms and for being unable to communicate with the inspectors. No lookouts or visa revocations were posted alerting border authorities to the terrorist association of two of the hijackers until after each has entered the United States for the last time.

Four hijackers were admitted after the secondary inspectors who interviewed them were

[3] *9/11 and Terrorist Travel* at p. 2
[4] Id. at p. 5-6

unable to, or did not, verify information supplied by the operative, misunderstood the law, or failed to follow procedures. One was interviewed at length by a border inspector. The inspector concluded, on the basis of his hostile and arrogant behavior and contradictory statements, that he was unlikely to comply with U.S. immigration law and posed a risk. He was denied entry. The inspector was backed up by his superior, but acted in the face of a general expectation of leniency toward Saudi citizens at that airport. These entries occurred during a period when approximately 20 million people applied for visas, and more than 10 million people came into the United States through 220 airports of entry.

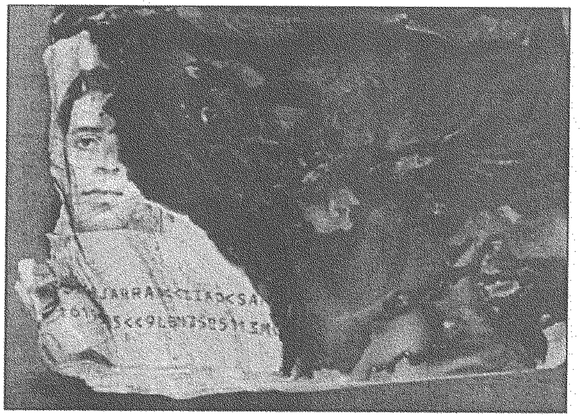
Terrorist Travel and Passports: Summary of *9/11 and Terrorist Travel* Findings

In the Al Qaeda Afghan training camps, we know that terrorists were well trained in travel and travel document forgery. Terrorists were instructed in how to move into Afghanistan through Iran or Pakistan, and what travel facilitators to use for acquiring travel documents and travel. Digital copies of travel documents were kept in e-files in safehouses (we obtained a couple of 9/11 hijacker passports from such files), and Adobe Photoshop was a favorite tool for manipulating multiple forms of identifications, including passports. Upon leaving training camps, Khalid Sheikh Mohammed (mastermind of the 9/11 plot) would instruct new recruits on how to behave to pass into the West unsuspected.

We know 9/11 operational ringleader Mohamed Atta used his training as well to manipulate passports to hide travel and substitute information that would leave a fraudulent trail of less suspicious travel by, for example, erasing stamps that showed travel in and out of Afghanistan. Atta performed this task for co-conspirator Ramzi Binalshibh. Al Qaeda also kept digital copies of passports of members, likely used, for example, to recycle necessary bits and pieces of deceased members' actual passports by substituting in new faces of active members for future travel.

For the terrorist, the underlying purpose of the travel will often determine how he decides to travel. For example, the nineteen 9/11 hijackers had a mission which required a relatively short time for legal admission into the United States, but also required that none of them be compromised for failure to obey immigration law. (Violations of law did exist; it was the federal government that failed to exercise its authority under the law.) Therefore, they needed to appear "clean" to immigration authorities.

They thus worked hard to appear to follow the rules. They all had passports. (Thirteen acquired new passports within three weeks prior to seeking U.S. visas. A number had indicators of extremism that remain classified today and still other passports contained fraudulent manipulations.) They all had visas (22 or 23 applications were approved). They all sought entry through immigration inspection kiosks at U.S. international airports (a total of 34 times over 21 months). In the five times 9/11 hijackers were pulled into secondary, only once did a hijacker resist questioning, and then quickly became cooperative once a new inspector was assigned to conduct the questioning. In two cases terror alerts or visa revocations were placed in the immigration system; but it was too late—in August 2001, subsequent to the last successful 9/11 hijacker entry in July 2001.[5]



A partly-burned copy of Ziad Jarrah's U.S. visa recovered from the Flight 93 crash site

In other words, the 9/11 hijackers had been taught what to do to attain successful entry into the United States. The frustrating irony is that at least some of the hijackers could have been denied admission into the United States if critical information had been provided to border officers via lookouts or regarding the passports themselves. Today, we have the ability to provide that information to our border security personnel *as long as a passport or verifiable biometric equivalent is required for admission.* However, where there is no passport or equivalent biometric travel document required for admission, as is the case as long as the Western Hemisphere Travel Exception is in place, our border personnel have little to no baseline upon which to make an initial judgment about whether a particular individual may pose a terrorist or public safety threat to the United States.

Nabil Al-Marabh

A good example of what occurs when inspections are done wholly randomly and without an inspector's training in the forensics of travel documents is the story of likely Al Qaeda member Nadil Al-Marabh. Al-Marabh stayed at a terrorist guesthouse in Pakistan known as the House of Martyrs, engaged in weapons training in Afghanistan, and worked for the Muslim World League—then an important source of al Qaeda's funds[6]—in the early 1990s.[7] He then worked at the same Boston cab company as individuals convicted in Jordan for the Millenium plot to blow up religious and western tourist locations in

[5] *9/11 and Terrorist Travel*, p. A-1.

[6] USA v. Arnaout. "Government's Evidentiary Proffer Supporting the Admissibility of Co-Conspirator Statements." NDIL 02-CR- 892. Jan. 31, 2003 at p. 25.

[7] Steve Fainaru. "Sept. 11 Detainee is Ordered Deported." The Washington Post. Sept. 4, 2002.

Jordan.[8] These individuals identified Al-Marabh as an al Qaeda operative.[9] Al-Marabh maintained a Boston address from 1989 to 2000.[10] He also lived in Toronto, Detroit, Tampa, and Chicago.[11]

On June 27, 2001, Al-Marabh tried to illegally enter the United States near Niagara Falls by hiding in the back of a tractor-trailer. He had a forged Canadian passport and fake social insurance card.[12] He later told authorities he had regularly traveled illegally between Canada and the United States.[13] Moreover, Michigan state records showed Al-Marabh receiving five driver's licenses there in thirteen months; he had licenses for Massachusetts, Illinois, Ontario, and Florida,[14] and a commercial driver's license and a permit to haul hazardous materials,[15] including explosives and caustic chemicals.[16]

In September 2001, authorities raided a Detroit residence that had Al-Marabh's name on the mailbox. They found three men with fake immigration documents, airport identification badges, and a notebook containing handwritten notes about security at a U.S. military base in Turkey and an airport in Jordan.[17] These men, who may also have been involved in a plot to kill former defense secretary William Cohen during a visit to Turkey,[18] were later charged with being part of an al Qaeda sleeper cell.[19] They were convicted, but the verdict was thrown out in September 2004.[20]

Al-Marabh was arrested in Chicago in September 2001 on a parole violation related to his stabbing of a man who had lived in his apartment.[21] In 2002, he pled guilty to conspiracy to smuggle an alien into the United States[22] and was ordered deported.[23] Prosecutors said

[8] Farmer, Tom. "Bin Ladin Operative May Have Lived In Dorchester For More Than 10 Years." The Boston Herald. Sept. 19, 2001 and USA. v. Elzahabi. DMN 04-MJ 26. "Criminal Complaint and Affidavit of Kiann Vandenover, FBI Special Agent." June 25, 2004.

[9] Golden, Tim with Judith Miller. "Bin Ladin Operative Is Linked To Suspects." The New York Times. Sept. 18, 2001.

[10] Farmer, Tom. "Bin Ladin Operative May Have Lived In Dorchester For More Than 10 Years." The Boston Herald. Sept. 19, 2001

[11] Schiller, Bill. "Terrorism Suspect had Florida Link." Toronto Star. Oct. 26, 2001.

[12] Dimmock, Gary and Aaron Sands. "Toronto Shop Clerk Tied to World Terror." The Ottawa Citizen. Oct. 29, 2001.

[13] Ibid.

[14] Schiller, Bill. "Terrorism Suspect had Florida Link." Toronto Star. Oct. 26, 2001.

[15] Philip Shenon and Don Van Natta Jr., "U.S. Says 3 Detainees May Be Tied to Hijackings," *The New York Times*, November 1, 2001.

[16] Wilgoren, Jody and Judith Miller. "Trail of Man Sought in 2 Plots Leads to Chicago and Arrest." New York Times. Sept. 21, 2001.

[17] USA v. Hannan, et al. EDMI 01-C-R80778. "Criminal Complaint of Robert Pertuso, FBI Special Agent." Sept. 18, 2001.

[18] "Terror Supporters among Us." Associated Press, Nov. 17, 2001. http://www.cbsnews.com/stories/2001/11/17/archive/main318417.shtml (accessed Oct. 28, 2004).

[19] USA v. Koubriti, et al. EDMI 01-C-R80778. Indictment. Sept. 27, 2001.

[20] Karush, Sarah. "Judge Drops Charges in Mich. Terror Case." The Associated Press. Sept.3, 2004.

[21] "Boston Fugitive Arrested." Federal Bureau of Investigation Press Release. Sept. 20, 2001. and Wilgoren, Jody and Judith Miller. "Trail of Man Sought in 2 Plots Leads to Chicago and Arrest." The New York Times. Sept. 21, 2001.

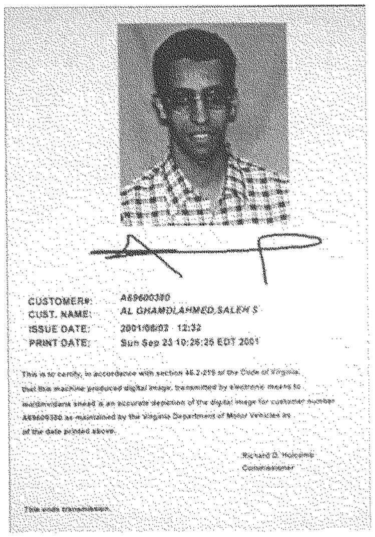
[22] USA v. Al-Marabh. WDNY 01-CR-244-A. Plea Agreement. July 8, 2002.

[23] Fainaru, Steve. "Sept. 11 Detainee is Ordered Deported." The Washington Post. Sept.4, 2002.

the government had no evidence linking him to terrorism.[24] The judge questioned the government's previous documentation of Al-Marabh's ties to terror and also noted he was found with $22,000 in cash and $25,000 worth of amber jewels in his possession when he was arrested.[25] He was deported to Syria in January 2004. Months later, a press release from Immigration and Customs Enforcement called Al-Marabh a "suspected terrorist."[26]

Driver Licenses

Fourteen of 15 operatives and all of the pilots acquired one or multiple forms of U.S. state-issued identification. Only Satam al Suqami did not, possibly because he was the only hijacker who knew he was out of immigration status: his length of stay end date of May 20, 2000, was clearly inserted in his passport. Six hijackers presented these documents to airline personnel on the morning of 9/11. We know all the Virginia identifications were acquired through fraud. Those stories are laid out in detail in the staff report.



CUSTOMER#: A69600380
CUST. NAME: AL GHAMDI,AHMED,SALEH S
ISSUE DATE: 2001/08/02 12:32
PRINT DATE: Sun Sep 23 10:28:25 EDT 2001

This is to certify, in accordance with section 46.2-215 of the Code of Virginia, that this machine produced digital image, transmitted by electronic means to [illegible] is an accurate depiction of the digital image for customer number A69600380 as maintained by the Virginia Department of Motor Vehicles as of the date printed above.

Richard D. Holcomb
Commissioner

This ends transmission.

Ahmed al Ghamdi's photo as it appeared on his state of Virginia identification card. Ziad Jarrah, Abdul Aziz al Omari and Salem al Hazmi also obtained Virginia state identification cards. The hijackers used false affidavits to obtain their identification.[27]

[24] Ibid.

[25] Owens, Anne Marie. "Judge Gets No Answers on Syrian: Former Toronto Suspect Jailed in U.S. for Border Breach." The National Post. Sept. 4, 2002.

[26] "Selected Terrorism Investigations That Involved ICE and ICE Authorities," Immigration & Customs Enforcement Press Release. July 27, 2004. http://www.ice.gov/graphics/news/factsheets/072704terrorist_fs.htm (accessed Oct. 5, 2004).

[27] *9/11 and Terrorist Travel*, p. A-24.

Identification Documents of the 9/11 Hijackers (*9/11 and Terrorist Travel*, p.44)

Mohamed Atta
FL DL, 05/02/01

Marwan al Shehhi
FL DL, 04/12/01
FL DL duplicate, 6/19/01

Khalid al Mihdhar
CA DL, 04/05/00
USA ID card, 07/10/01
VA ID card, 08/01/01

Nawaf al Hazmi
CA DL, 04/05/00
FL DL, 06/25/01
USA ID card, 07/10/01
VA ID card, 08/02/01

Hani Hanjour
AZ DL, 11/29/91
FL ID card, 04/15/96
VA ID card, 08/01/01
Failed VA DL test, 08/02/01
MD ID card, 09/05/01

Ziad Jarrah
FL DL, 05/02/01
FL DL duplicate 5/24/01
VA ID card, 08/29/01

Satam al Suqami
No DL or ID card

Waleed al Shehri
FL DL, 05/04/01
(duplicate issued with different address, 05/05/01)

Ahmed al Ghamdi
USA ID card, 07/2001
VA ID card, 08/02/2001

Majed Moqed
USA ID card, 07/2001
VA ID card, 08/02/2001

Hamza al Ghamdi
FL ID card, 06/26/01
FL DL, 07/02/01
(duplicate issued 08/27/01)

Mohand al Shehri
FL ID card, 07/02/01

Ahmed al Nami
FL DL, 06/29/01

Wail al Shehri
FL DL, 07/03/01

Ahmed al Haznawi
FL DL, 07/10/00
(duplicate issued 09/07/01)

Fayez Banihammad
FL ID, 07/10/01

Saeed al Ghamdi
FL ID card, 07/10/01

Salem al Hazmi
USA ID card, 07/01/01197
VA ID card, 08/02/01

Abdul Aziz al Omari
USA ID card, 07/10/2001
VA ID card, 08/02/2001

Driver licenses are also a chosen method of entry into the United States. Take the example of the D.C. area snipers, John Lee Muhammed and Lee Boyd Malvo. John Lee Mohammed, the U.S. citizen responsible for 10 fatal shootings and 3 other near fatal shootings during a terrorist-style spree in the autumn of 2002, had financially survived prior to coming to the United States by selling forged U.S.-accepted travel documents—driver's licenses and birth certificates in Antigua and Baruba.

Muhammed brought Lee Boyd Malvo and his three children into the United States under false names, and in at least 20 incidents forged or stole identities for clients, secured air travel, and provided documents in order to secure their travel to the United States. In some cases, he charged as much as $3,000. He forged documents for Lee Boyd Malvo's mother when she deserted her son, but when he was not paid, Muhammed kept Malvo as collateral.

With simply a birth certificate or baptismal record and a driver's license, Mohammed's clients, covered by the Western Hemisphere Exception for travelers from North, South or Central America or the Caribbean (but for Cuba), could easily pose as American citizens or citizens of one of the covered nations, and enter the United States.[28]

GAO's Most Recent Findings

GAO's most recent findings regarding border inspection at a variety of land and air ports of entry on the north, south and east coasts of the United States highlight three important issues.

- **Not much has changed since 9/11.** The 9/11 hijackers were successfully able to enter the United States a total of 34 of 35 attempts (a 97 % success rate). Between 45 attempted entries by GAO between 2003 and 2006, 42 of 45 attempts (a 93% success rate) at entries were successful with even less acceptable documentation than a standard passport and visa, which the 9/11 hijackers did possess. A reasonable conclusion then, that there is little disincentive to presenting a fake document, as there is an over 90% chance at success and no chance it will be vetted like a passport is.
- Border inspectors still **operate under old policies and procedures** that emphasize customer service over security, and often provide ineffective security at our border ports of entry. For example, the Western Hemisphere Exception permits presentation of any of thousands of "identity" documents produced anywhere in the Western Hemisphere for citizens of the Western Hemisphere as legitimate identity/travel documents.
- There remains **significant laxity in our border inspection processing**, most acute at land ports of entry. Time allotted to process travelers varies from port to port—generally still in the one-minute range at air ports of entry, but at land ports of entry, checks are still random and many are not checked at all.
- Where border inspectors do conduct checks of documents, they lack the **time, training, technology** and **access to information** to make consistent distinctions between legitimate and fraudulent documentation amongst the thousands of

[28] Antigua and Barbuda Final Report of Task Force Investigation of John Allen Williams, a.k.a John Allen Mohammad. December 2003.

varieties of identification documentation acceptable for presentation under the Western Hemisphere Exception.

- CBP has duplicated the efforts of the Forensic Document Lab (now located at ICE) by providing expensive machines in secondary inspection while not providing all primary inspectors with basic tools to do their jobs.
- CBP is cross training new inspectors in customs and immigration law, both of which are highly complex, while providing minimal training on forensics in documents in basic training. Such training still takes place at ports of entry "on the line", for the most part.
- Basic information that should be available at primary inspections is still not available. This includes the declassification of terrorist indicator information on passports that I believe is still is not available to inspectors today and access to Interpol's real time lost and stolen passport database to primary inspectors.

The 9/11 Commission Recommendation Regarding Passports or a Biometric Equivalent

In a now oft-repeated quote from the *9/11 Final Report*, we summarized our findings based on 18 months of research into how the 9/11 hijackers got in and stayed in the United States as follows:

> For terrorists, travel documents are as important as weapons. Terrorists must travel clandestinely to meet, train, plan, case targets, and gain access to attack. To them, international travel presents great danger, because they must surface to pass through regulated channels, present themselves to border security officials, or attempt to circumvent inspection points.
>
> In their travels, terrorists use evasive methods, such as altered and counterfeit passports and visas... immigration and identity fraud. These can sometimes be detected. (p. 384)

The Report continues later with clear recommendations:

> Americans should not be exempt from carrying biometric passports or otherwise enabling their identities to be securely verified when they enter the United States; nor should Canadians or Mexicans. Currently U.S. persons are exempt from carrying passports when returning from Canada, Mexico, and the Caribbean. They current system enables non-U.S. citizens to gain entry by showing minimal identification. The 9/11 experience shows that terrorists study and exploit America's vulnerabilities.
>
> To balance this measure, programs to speed known travelers should be a higher priority, permitting inspectors to focus on greater risks. The daily commuter should not be subject to the same measures as first-time travelers. An individual should be able to pre-enroll, with his or her identity verified in passage. Updates of database information and other checks can ensure ongoing reliability. (p. 388)

In making this recommendation, the Commission drew on intensive research not just about the 9/11 hijackers, but the pre-9/11 terrorists whose immigration files we were able to review in depth. Since then, I pursued a further study published by the Center for Immigration Studies in August 2005 which detailed how 94 terrorists (including six of the 9/11 hijackers) had abused our immigration benefits system to embed either permanently or for long periods of time. That paper, entitled *Immigration and Terrorism: Moving Beyond the 9/11 Staff Report on Terrorist Travel*, makes it clear that successful terrorist entry by any means- whether a tourist or business visa, student visa, or request for political asylum or naturalization- will have a high likelihood of attaining permanent residency and naturalization when sought. Naturalization, in turn, is an automatic access to a U.S. passport.

New laws addressing terrorist travel

National Intelligence Reform Act of 2004

I wish to applaud Congress for passing the National Intelligence Reform Act of 2004, and the Chairman and the members of this committee that voted for it. That law contains many important terrorist travel provisions, including provisions providing for more robust screening procedures at ports of entry and the new passport rules that are both the subject of today's hearing. I look forward to working with this Committee in supporting the need to implement this law in step with the *9/11 Final Report* recommendations.

The rollout for the Western Hemisphere Travel Initiative is as follows:

1. December 31, 2006 – Requirement applied to all air and sea travel to or from Canada, Mexico, Central and South America, the Caribbean, and Bermuda.
2. December 31, 2007 – Requirement extended to land border crossings as well as air and sea travel.

A two-tiered rollout is absolutely essential. Kinks in implementing the Initiative can be worked out prior to execution at the land border ports of entry, which experience higher volumes of incoming applicants alongside commercial, and commuter traffic. A delayed roll-out until the statutory deadline of January 1, 2008 will not only unnecessarily impact our national security, but will nearly assure a bureaucratic death for a new program which requires both the technology and the border officers to work seamlessly in practice.

Working within the mandate of the Intelligence Reform Act, the State Department is working on alternatives to a passport for the communities adjacent to our physical borders with Canada and Mexico. To accommodate the concerns expressed in the hundreds of comments on the rulemaking, the State Department is planning to introduce a Department of State-produced Passport Card that can act as a U.S. passport in an alternative format with all the security features and vetting of a U.S. passport. DHS and State have agreed that the biometric taken will be the same as for a U.S. passport, a facial image.

As planned, it will be available at the 7,000 offices that already process passports and cost about half as much as a U.S. passport. It will look much like a driver's license and fit into a wallet, but will not actually contain biometrics (identity) and registration information (citizenship). Instead, it will link back into a State/DHS database that will verify the cardholder with the card information (thereby protecting privacy).

The Passport Card will also serve as a platform to which DHS can add privileges for registered travelers. If the traveler wants to add these "privileges", Customs and Border Protection will need to collect 10 fingerscans, and conduct a full criminal background check and an interview. Again, those "privileges" will be registered in a joint run DHS-State database, not the card, and can expire or be revoked by DHS. The biometric feature will allow DHS to identify the benefits to which the traveler is entitled. Along with this card, NEXUS (northern border commuters), SENTRI (southern border commuters) and FAST (northern border commercial drivers), and the Border Crossing Card (Mexican laser visa) will also likely be an acceptable as a substitute for a passport and a visa for traveling to the United States from North or South America, including the Caribbean.

This card will be a better selling point to the border communities and others who will benefit from it if and when DHS and the State Department must resolve if and how RFID technology will be added to it, or whether those with the travel card will have dedicated lanes. A traveler will then not only have the added value of an easy carrying and cheaper option for a passport, but also have the added value of possession of the card truly facilitating entry at land POEs. With the proper physical and technological infrastructure and human resources in place, the potential for increasing security and facilitating trade and travel is manifold.

It is positive to see the Immigration Reform Act of 2006 embracing the card.

Addressing Concerns About Ramped Up Border Inspection

Today, there is much concern that ramped up border inspection, including implementation of WHTI, is going to substantially impede the flow of trade and tourism across ports of entry. These concerns (*in italics below*), can be addressed as follows:

1. *Passports or an approved equivalent will significantly slow down traffic at POEs.* Not so. If we give border inspectors the tools they need to do their job efficiently and effectively, the implementation of WHTI can be painless, taking away from the border inspector the need to question and review in depth (and never verify) the authenticity of thousands of varieties of birth certificates (about 50,000 in the US today) and driver licenses (about 240 varieties today) down to a passport or equivalent that verifies-- at a much lower rate of fraud- citizenship and identity with the right tools to get the job done.
2. *That security is sufficiently achieved by retaining random checks of vehicles and their passengers at land POEs.* The GAO study makes it clear that random checks mean no checks of some and insufficient checks of others provides minimal, and often no security whatsoever.

3. *RFID technology and the type of RFID applied, and by whom, is the key to operationally implement WHTI.* That simply is not the case. Different courses of action should be pre-tested with a variety of technologies and use of that technology with a variety of lane and personnel uses—e.g. by maximizing the best combination of technologies with physical infrastructures and personnel at POEs, we can mitigate much of the potential concern about ramped up border security slowing down trade and tourism.

Nexus and FAST

Streamlining the admission process for low risk travelers augments U.S. national security by permitting the immigration and customs officers who enforce U.S. immigration law at the border to focus on those seeking entry who may pose a national security risk. This does not mean that sleeper cell style terrorists could not exploit, for example, NEXUS and FAST, on the northern border or SENTRI on the southern border. Of course they could. However, there is little incentive for them to risk being vetted in watchlists and criminal databases and having an enrollment in a U.S. government program that could highlight their identity, freezes their biometric and travel patterns. The result is that programs like these, as long as they are tamper proof on a number of levels, should be sufficient to replace the passport as a viable biometric travel document. Our *9/11 Final Report* and the findings of my team's *9/11 and Terrorist Travel* both support that conclusion.

In addition, these programs—once they have achieved a threshold of enrollment-- are proving their worth in cutting down wait times at northern land ports of entry for all entrants, siphoning off the SENTRI, NEXUS and FAST drivers and passengers into dedicated lanes and allowing wait times for remaining travelers to be reduced as well. Right now, SENTRI exists at three locations on the southern border with 30 lanes operating and NEXUS exists at 12 land border ports of entry and has 15 lanes. FAST is in place at 35 land ports of entry and has 136 dedicated lanes. Canadian NEXUS now exists at eight land border ports of entry for commerce flowing from the United States into Canada. NEXUS has reduced processing time from a potential stop by a border officer to a guaranteed five to seven second crossing time once at the border station.

The result is that commerce—in terms of commuter and commercial traffic, as well as tourism- is enhanced across the board, a win-win situation. Americans commuting to Canada will find a similar upgrade in their wait times when the Canadians expand their version of NEXUS, with a contract just recently awarded for a Canadian NEXUS to be developed further and installed over the next few years. We must work to insure that NEXUS, FAST and SENTRI are easily available to those who seek to enroll, and that the ports are configured to maximize the benefits of the program.

REAL ID Act of 2005

I also want to thank Congress for their work in making driver licenses meet minimum standards of identity verification and document authenticity. The REAL ID Act was passed in large part to counter the ease with which the 9/11 hijackers attained 14 driver licenses and 10 state issued identifications from California, Florida, Maryland and Virginia.[29] We know that at least six hijackers presented these ids on the morning of 9/11 to disguise their lack of affiliation with the United States.[30]

The policy behind the REAL ID Act is to make it more difficult for terrorists and those who seek to circumvent U.S. laws to embed in the United States. The law brings driver licenses and state-issued identifications issued within the United States closer in step (although not completely) with our latest requirements for secure and verifiable travel documents for entry into the United States. If Congress wants to have U.S. issued state driver licenses pass muster as a "biometric equivalent" to a U.S. passport, we must all understand what that would mean. Congress would have to be willing to step up to fund REAL ID in a manner that makes U.S. driver licenses machine readable at ports of entry so that the license was scanable; could automatically verify identity and citizenship; be vetted for security; and authenticate both driver license and immigration status. In other words, the driver license would need to interact and act in partnership with the federally issued U.S. passport.

With over 240 varieties of state-issued driver licenses, one important reason for implementing WHTI is to streamline the inspector's time and enable forensic subject matter expertise. A single document like the passport can be trained for forensic review by border inspectors. In juxtaposition, we can never ask border inspectors to verify 240 varieties of driver licenses (or even 50 for that matter) in the 45 second time frame that most inspectors are allocated to adjudicate an applicant seeking admission into the United States unless the inspectors are given the training, tools and sufficient information to make that inspection occur quickly and adequately.

9/11 Commission Terrorist Travel Recommendations Remain Valid

Today, terrorists with Canadian, Caribbean or Mexican citizenship can move in and out of the United States virtually unconcerned about detection. There are legitimate concerns about both the northern, southern and sea borders. And with a growing group of jihadists in Canada, Trinidad and Venezuela openly supporting terrorist activity and clandestine movement of terrorists, the Tri-border area in South America known for fraudulent document production and a volatile Mexican border ripe with smuggling activities, and an embedded Hizballah contingent within the United States, we cannot underestimate the value of deploying the most efficient and effective border security technology, training and information-access to our border personnel on our physical borders and at our ports of entry.[31] Ramped up border security that provides border inspectors what they need in

[29] See *9/11 and Terrorist Travel: A Staff Report of the National Commission on Terrorist Attacks Upon the United States* (Franklin, Tenn.: Hillsboro Press, 2004) at p. 44. It is available in book form at http://providence-publishing.com/Merchant2/merchant.mvc?Screen=PROD&Store_Code=PP&Product_Code=9ATT&Category_Code=FTANR.

[30] Ibid at p. 43.

[31] My testimony before the House Committee on the Judiciary Subcommittee on Immigration, Border Security, and Claims, Oversight Hearing on "The Need to Implement WHTI to Protect U.S. Homeland Security" June 8, 2006. I also testified on November 17, 2005 before the House Small Business Committee, "Building a Wall Between Friends: Passports to and from Canada?"

time, technology, training, information and policy thus becomes essential to chilling terrorist travel between the U.S. and Canada/Mexico and the Caribbean. This includes any terrorist, whether a Mexican Islamic convert (as sought out by Al Qaeda) or Canadian or third country national posing as a citizen of the Western Hemisphere. Terrorists do not like to be detected or detectable, nor do they want their identity "frozen". (We know, for example, from detainee reporting after 9/11, that the tightening of immigration admission standards for persons traveling from countries of interest resulted in Al Qaeda leaders seeking out young recruits and others with easy access to the West—U.S. citizens, Canadians, Mexicans and those with access to Visa Waiver passports.)

Even if terrorists choose to acquire a passport with a false identity and with false underlying support documents (as Ahmed Ressam did) that identity is at least frozen and aliases to cross the border (as Ressam did use) are not possible. What would have caught Ressam was a biometric in that passport that then linked up to the watchlist Ressam was indeed listed on in Canada. Today, a hit on a terrorist such as Ressam would most likely occur through either a DHS TECS Lookout provided by U.S. or foreign law enforcement, a U.S. terror watchlist hit, an IDENT or FBI IAFIS hit, or through a biometric wanted notice now available to our border inspectors through Interpol.

9/11 and Terrorist Travel details in great depth how the 9/11 hijackers exploited our vulnerabilities using our legal border system and in our state-issued driver license regime. Part of the everyday business of terrorist travel is the bustling black market in doctored and false passports and other false or illegally obtained identity documents. In addition, an estimated 10 million lost or stolen passports or national identification cards worldwide afford terrorists easier access to world travel.[32] This permits easy travel based on aliases, fake or stolen identities that, at a land border, may or may not be subject to a database check. Requiring U.S. citizens to carry a passport or biometric equivalent also means U.S. border inspectors no longer need to play a guessing game as to who is and who is not a U.S. citizen. On the borders, having a combination of the standard passport or equivalent and registered traveler programs that limit what a border officer must review gives border officers a better chance of snuffing out Canadian, Mexican or other Western Hemisphere passports that might be fake or stolen.

Conclusion

As I have testified on a number of occasions, our U.S. border security is in dire shape. However, there are a few bright lights. Along with the entry portion of U.S. Visit in place and a new emphasis on increasing interior and physical border law enforcement under the Secure Border Initiative, ramping up border inspection now while working to implement WHTI is a essential to fulfilling the first and foremost requirement of border security—to provide security at our borders against terrorist entry and embedding and cross-border terrorist travel traffic. Stopping terrorist entry and embedding must be a high priority objective.

[32] Levine, Samantha. "Terror's Best Friend." US News & World Report. December 6, 2004.

However, that does not mean it need be achieved to the exclusion of commerce; it need not be. In fact, facilitation of low risk travelers and commerce is a necessary step in enhancing border officers' ability to focus on higher risk applicants for entry into the United States.

To break down the national security policy implications further of the effect that the Western Hemisphere Travel Initiative will have on the terrorist, here are the options that exist for a terrorist today: (1) use a legitimate passport using his or her real name and risk showing up on a database check; (2) use a whole variety of other documentation such as driver licenses or birth certificates that can be neither verified for content nor authenticated as government issued documents yet permits a "clean" entry; or (3) enter illegally over the physical borders. For the terrorist today, the most optimum form of travel, then, is to use option (2), identification that can neither be authenticated nor its contents verified and contains no biometrics. By eliminating option (2), the terrorist now has to make a choice: either risk exposure to the government of his identity and whereabouts or enter illegally. Requiring use of a biometrically based passport under option (1) is what the United States needs to do to lower its risk of terrorist entry. In regard to option (3), we must take measures against illegal entry as soon as possible. There is reason for concern here, however, as Secretary Chertoff's recently announced Secure Border Initiative almost singularly focuses on the southwest border and current rumblings within the administration keep setting back making a decision on a due date for implementation.

The lesson learned from study of pre-9/11, 9/11 and post 9/11 terrorists is that verifying identification, appropriately conducting a security check on that identification, and authenticating travel documents are all absolutely essential at all stages of contact with the U.S. border apparatus—whether it be in a consulate office abroad, at a port of entry, or an immigration benefit office. However, since the port of entry is the last chance to prevent *physical* entry into the U.S. where a series of other rights seem to accrue once in the U.S. under practice, the port of entry becomes the crucial last place to prevent terrorist entry into the United States.

As the terrorist conspiracy in Ontario with U.S. links and established cross border traffic between terrorists in the United States with Canada established, our national security might indeed depend on just that. If Congress fails to insist that DHS (in concert with the State Department) ramp up border security *now*, the result will be that terrorists and criminals will continue to be able to enter the United States unfettered on forged documents such as birth certificates and driver licenses until it is in place. Is that worth a delay? No. Can we do things now to help assure more accurate screening until implementation in another year and a half? I believe so, but it will take the will of Congress in both oversight and budget to make it happen. I hope this hearing will provide such impetus.

United States Government Accountability Office

GAO

Testimony
Before the Committee on Finance,
U.S. Senate

For Release on Delivery
Expected at 10:00 a.m. EDT
Wednesday, August 2, 2006

BORDER SECURITY

Continued Weaknesses in Screening Entrants into the United States

Statement of Gregory D. Kutz, Managing Director
Forensic Audits and Special Investigations

GAO
Accountability * Integrity * Reliability

Mr. Chairman and Members of the Committee:

Thank you for the opportunity to be here today to discuss our investigation of the effectiveness of U.S. Customs and Border Protection (CBP) in screening entrants into the United States at land border crossings. Currently, U.S. citizens are not required to present a passport when entering the United States from countries in the Western Hemisphere.[1] However, U.S. citizens are required to establish citizenship to a CBP officer's satisfaction.[2] On its Web site, CBP advises U.S. citizens that an officer may ask for identification documents as proof of citizenship, including birth certificates or baptismal records and a photo identification document.[3]

In 2003, we testified that CBP officers were not readily capable of identifying whether individuals seeking entry into the United States were using counterfeit identification to prove citizenship. Specifically, our agents were able to easily enter the United States from Canada and Mexico using fictitious names and counterfeit driver's licenses and birth certificates.[4] Later in 2003 and 2004, we continued to be able to successfully enter the United States using counterfeit identification at land border crossings, but were denied entry on one occasion.

Specifically, agents entered the United States using counterfeit driver's licenses at two land crossings in Washington, one in New York, one in California, and one in Texas. One agent was also able to enter the United States through both the California and Texas border crossings using an expired, altered U.S diplomatic passport. CBP officers did not question the authenticity of these agents' identification. Furthermore, at one of the Washington crossings, agents were able to walk across the border without passing through any security checkpoints and without presenting identification. However, another agent who entered at the New York crossing was not allowed entry into the United States after presenting as identification an expired, altered U.S. tourist passport and a counterfeit

[1] 22 C.F.R. § 53.2(b).

[2] 8 C.F.R. § 235.1(b).

[3] See http://www.cbp.gov/xp/cgov/travel/vacation/documentary_requirements.xml.

[4] We also testified in 2003 that agents successfully entered Florida from Jamaica via air. GAO, *Weaknesses in Screening Entrants into the United States*, GAO-03-438T (Washington, D.C.: Jan. 30, 2003).

driver's license. CBP officers detained this agent for further screening until he identified himself as a GAO employee conducting undercover tests. [5]

Because of your concerns that these weaknesses could possibly be exploited by terrorists or others involved in criminal activity, you requested that we assess the current status of security at the nation's borders. Specifically, you requested that we conduct a follow-up investigation to determine whether the vulnerabilities exposed in our prior work continue to exist.

To perform our 2006 follow-up investigation, we created a fictitious driver's license and birth certificate with the same name that we used in the tests conducted for the work we did in 2003. We also created another fictitious license and birth certificate. To create all these documents, we used commercial software that is available to the public. As agreed with your offices, we chose to test a nonrepresentative selection of nine land crossings at both the northern and southern borders, including one in California, one in Texas, two in Arizona, one in Michigan, two in New York, one in Idaho, and one in Washington. We conducted our work from February 2006 through June 2006 in accordance with the President's Council on Integrity and Efficiency Quality Standards for Investigations.

Summary

Agents successfully entered the United States using fictitious driver's licenses and other bogus documentation through nine land ports of entry on the northern and southern borders. CBP officers never questioned the authenticity of the counterfeit documents presented at any of the nine crossings. On three occasions—in California, Texas, and Arizona—agents crossed the border on foot. At two of these locations—Texas and Arizona—CBP allowed the agents entry into the United States without asking for or inspecting any identification documents.

After completing our investigation, we briefed officials from CBP on June 9, 2006. CBP agreed that its officers are not able to identify all forms of counterfeit identification presented at land border crossings and fully supports a new initiative that will require all travelers to present a

[5] As part of this investigation, agents also attempted to enter the Unites States via air. Agents successfully entered the United States from the Bahamas using counterfeit driver's licenses and birth certificates. However, agents were not successful when attempting to enter the United States from Jamaica; CBP officers detained four agents in Florida until they identified themselves as GAO employees conducting tests.

passport before entering the United States. We did not assess whether this initiative would be effective in preventing terrorists from entering the United States or whether it would fully address the vulnerabilites shown by our work.

Southern Border Crossings

The following information provides details about our agents' experiences and observations entering the United States from Mexico at border crossings in California and Texas and at two crossings in Arizona.

California: On February 9, 2006, two agents entered California from Mexico on foot. One of the agents presented as identification a counterfeit West Virginia driver's license and the other presented a counterfeit Virginia driver's license. The CBP officers on duty asked both agents if they were U.S. citizens and both responded that they were. The officers also asked the agents if they were bringing anything into the United States from Mexico and both answered that they were not. The CBP officers did not request any other documents to prove citizenship, and allowed both agents to enter the United States.

Texas: On February 23, 2006, two agents crossed the border from Mexico into Texas on foot. When the first agent arrived at the checkpoint, a CBP officer asked him for his citizenship information; the agent responded that he was from the United States. The officer also asked if the agent had brought back anything from Mexico. The agent responded that he had not, and the officer told him that he could enter the Unites States. At this point, the agent asked the CBP officer if he wished to see any identification. The officer replied "OK, that would be good." The agent began to remove his counterfeit Virginia driver's license from his wallet and the inspector said "That's fine, you can go." The CBP officer never looked at the driver's license.

When the second agent reached the checkpoint, another CBP officer asked him for his citizenship information and he responded that he was from the United States. The CBP officer asked the agent if he had purchased anything in Mexico and the agent replied that he had not. He was then asked to show some form of identification and he produced a counterfeit West Virginia driver's license. The CBP inspector briefly looked at the driver's license and then told the agent he could enter the United States.

Arizona, first crossing: On March 14, 2006, two agents arrived at the border crossing between Mexico and Arizona in a rental vehicle. Upon request, the agents gave the CBP officer a counterfeit West Virginia driver's license and counterfeit Virginia driver's license as identification. As the CBP officer reviewed the licenses, he asked the agents if they were U.S. citizens and they responded that they were. The officer also asked if the agents had purchased anything in Mexico and they said they had not. The CBP officer then requested that agents open the trunk of their vehicle. The agents heard the inspector tap on several parts of the side of the vehicle first with his hand and again with what appeared to be a wand. The officer closed the trunk of the vehicle, returned the agents' driver's licenses, and allowed them to enter the United States.

Arizona, second crossing: On March 15, 2006, two agents again entered Arizona from Mexico on foot at a different location than the previous day. One of the agents carried a counterfeit West Virginia driver's license and a counterfeit West Virginia birth certificate. The other carried a counterfeit Virginia driver's license and a counterfeit New York birth certificate. As the agents were about to cross the border, another agent who had crossed the border earlier using his genuine identification phoned to inform them that the CBP officer on duty had swiped his Virginia driver's license through a scanner. Because the counterfeit driver's licenses the agents were carrying had fake magnetic strips, the agents decided that in the event they were questioned about their licenses, they would tell the CBP officers that the strips had become demagnetized.

When the agents entered the checkpoint area, they saw that they were the only people crossing the border at that time. The agents observed three CBP officers on duty; one was manning the checkpoint and the other two were standing a short distance away. The officer manning the checkpoint was sitting at a cubicle with a computer and what appeared to be a card scanner. The agents engaged this officer in conversation to distract him from scanning their driver's licenses. After a few moments, the CBP officer asked the agents if they were both U.S. citizens and they said that they were. He then asked if they had purchased anything in Mexico and they said no. He then told them to have a nice day and allowed them to enter the United States. He never asked for any form of identification.

Northern Border Crossings

The following information provides details about our agents' experiences and observations entering the United States from Canada at Michigan, New York, Idaho, and Washington border crossings.

Michigan: On May 1, 2006, two agents drove in a rental vehicle to a border crossing in Michigan. When asked for identification by the CBP officer on duty, the agents presented a counterfeit West Virginia driver's license and a counterfeit Virginia driver's license. As the CBP officer examined the licenses, he asked the agents if they were U.S. citizens and they responded that they were. The CBP officer then asked if the agents had birth certificates. One agent presented a counterfeit New York birth certificate and the other presented a counterfeit West Virginia birth certificate. The agents observed that the CBP officer checked the birth certificates against the driver's licenses to see if the dates and names matched. The CBP officer then asked the agents if they had purchased anything in Canada and they responded that they had not. The officer also asked what the agents were doing in Canada and they responded that they had been visiting a casino in Canada. The CBP officer then returned the agents' documentation and allowed them to enter the United States.

New York, first crossing: On May 3, 2006, two agents entered New York in a rental vehicle from Canada. The agents handed the CBP officer on duty counterfeit driver's licenses from West Virginia and Virginia. The CBP officer asked for the agents' country of citizenship and the agents responded that they were from the United States. The CBP officer also asked the agents why they had visited Canada. The agents responded that they had been gambling in the casinos. The CBP officer told the agents to have a nice day and allowed them to enter the United States.

New York, second crossing: On the same date, the same two agents crossed back into Canada and re-entered New York at a different location. The agents handed the CBP officer at the checkpoint the same two counterfeit driver's licenses from West Virginia and Virginia. The officer asked the agents what they were doing in Canada and they replied that they been gambling at a casino. The officer then asked the agents how much money they were bringing back into the country and they told him they had approximately $325, combined. The officer next asked the agent driving the car to step out of the vehicle and open the trunk. As the agent complied, he noticed that the officer placed the two driver's licenses on the counter in his booth. The officer asked the agent whose car they were driving and the agent told him that it was a rental. A second officer then asked the agent to stand away from the vehicle and take his hands out of his pockets. The first officer inspected the trunk of the vehicle, which was empty. At this point, the officer handed back the two driver's licenses and told the agents to proceed into the United States.

Idaho: On May 23, 2006, two agents drove in a rental vehicle to a border crossing in Idaho. The agents handed the CBP officer on duty a counterfeit West Virginia driver's license and a counterfeit Virginia driver's license. As the CBP officer examined the licenses, he asked the agents if they were

U.S. citizens and they responded that they were. The CBP officer then asked if the agents had birth certificates. One agent presented a counterfeit New York birth certificate and the other presented a counterfeit West Virginia birth certificate. The agents observed that the CBP officer checked the birth certificates against the driver's licenses to see if the dates and names matched. The officer also asked what the agents were doing in Canada and they responded that they had been sightseeing. The CBP officer then returned the agents' documentation and allowed them to enter the United States.

Washington: On May 24, 2006, two agents drove in a rental vehicle to a border crossing checkpoint in Washington. When the agents arrived at the border, they noticed that no one was at the checkpoint booth at the side of the road. Shortly thereafter, a CBP officer emerged from a building near the checkpoint booth and asked the agents to state their nationality. The agents responded that they were Americans. The CBP officer next asked the agents where they were born, and they responded New York and West Virginia. The agents then handed the CBP officers their counterfeit West Virginia and Virginia driver's licenses. The officer looked at the licenses briefly and asked the agents why they had visited Canada. The agents responded that they had a day off from a conference that they were attending in Washington and decided to do some sightseeing. The CBP officer returned the agents' identification and allowed them to enter the United States.

Corrective Action Briefing

We conducted a corrective action briefing with officials from CBP on June 9, 2006, about the results of our investigation. CBP agreed its officers are not able to identify all forms of counterfeit identification presented at land border crossings. CBP officials also stated that they fully support the newly promulgated Western Hemisphere Travel Initiative,[6] which will require all travelers, including U.S. citizens, within the Western Hemisphere to have a passport or other secure identification deemed

[6] See Western Hemisphere Travel Initiative, 70 Fed Reg. 52037.

sufficient by the Secretary of Homeland Security[7] to enter or reenter the United States. The current timeline proposes that the new requirements will apply to all land border crossings beginning on December 31, 2007. The proposed timeline was developed pursuant to the Intelligence Reform and Terrorism Prevention Act of 2004. The act requires the Secretary of Homeland Security, in consultation with the Secretary of State, to implement a plan no later than January 1, 2008, to strengthen the border screening process through the use of passports and other secure documentation in recognition of the fact that additional safeguards are needed to ensure that terrorists cannot enter the United States.[8] However, the Senate recently passed a bill to extend the implementation deadline from January 1, 2008, to June 1, 2009. Additionally, the Senate bill would also authorize the Secretary of State, in consultation with the Secretary of Homeland Security, to develop a travel document known as a Passport Card to facilitate travel of U.S. citizens to Canada, Mexico, the countries located in the Caribbean, and Bermuda.[9] We did not assess whether this initiative would be fully implemented by either the January 2008 or June 2009 deadline or whether it would be effective in preventing terrorists from entering the United States.

Conclusion

The results of our current work indicate that (1) CBP officers at the nine land border crossings tested did not detect the counterfeit identification we used and (2) people who enter the United States via land crossings are not always asked to present identification. Furthermore, our periodic tests since 2002 clearly show that CBP officers are unable to effectively identify counterfeit driver's licenses, birth certificates, and other documents. This vulnerability potentially allows terrorists or others involved in criminal activity to pass freely into the United States from Canada or Mexico with

[7] Although a passport will be the preferred form of identification for entry into the United States, the Department of State and CBP anticipate that other acceptable forms of identification will be the Border Crossing Card (BCC or laser visa), the Customs and Border Protection Secure Electronic Network for Travelers Rapid Inspection (SENTRI), NEXUS, and Free and Secure Trade (FAST) program cards. BCC cards have a photo and machine-readable biometric information; SENTRI cards are used for the automated commuter lanes at the United States/Mexico border crossings; NEXUS cards are issued to low-risk travelers for travel between Canada and the United States; and FAST cards are used by low-risk truck drivers, carriers, and importers at the United States/Canada border crossings.

[8] Pub. L. No. 108-458, § 7209, 118 Stat. 3638, 3823 (2004).

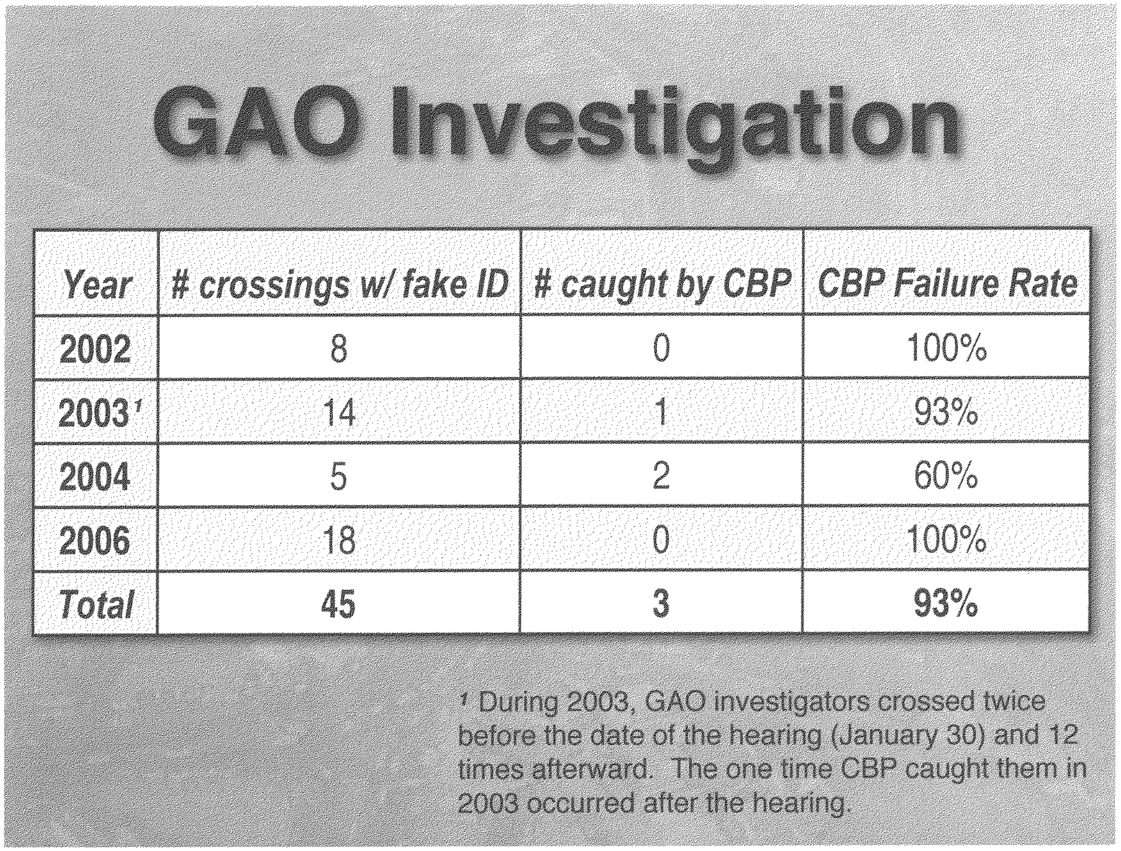
[9] Comprehensive Immigration Reform Act of 2006, S. 2611, 109th Cong. §135.

little or no chance of being detected. It will be critical that the new initiative requiring travelers within the Western Hemisphere to present passports or other accepted documents to enter the United States address the vulnerabilities shown by our work.

Mr. Chairman and Members of the Committee, this concludes my statement. I would be pleased to answer any questions that you may have at this time.

Contact

For further information about this testimony, please contact Gregory D. Kutz at (202) 512-7455 or kutzg@gao.gov. Contact points for our Offices of Congressional Relations and Public Affairs may be found on the last page of this testimony.



GAO Investigation

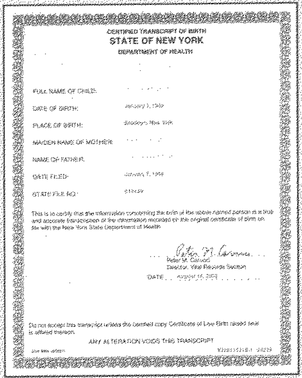
Year	*# crossings w/ fake ID*	*# caught by CBP*	*CBP Failure Rate*
2002	8	0	100%
2003[1]	14	1	93%
2004	5	2	60%
2006	18	0	100%
Total	**45**	**3**	**93%**

[1] During 2003, GAO investigators crossed twice before the date of the hearing (January 30) and 12 times afterward. The one time CBP caught them in 2003 occurred after the hearing.

Forensic Audits and Special Investigations

GAO
Accountability * Integrity * Reliability

Counterfeit Documents Used to Gain Entry to the United States



CERTIFIED TRANSCRIPT OF BIRTH
STATE OF NEW YORK
DEPARTMENT OF HEALTH

FULL NAME OF CHILD:

DATE OF BIRTH: [illegible]

PLACE OF BIRTH: Brooklyn, New York

MAIDEN NAME OF MOTHER:

NAME OF FATHER:

DATE FILED: [illegible]

STATE FILE NO: [illegible]

This is to certify that the information concerning the birth of the above named person is a true and accurate transcription of the information recorded on the original certificate of birth on file with the New York State Department of Health

Director, Vital Records Section

DATE [illegible]

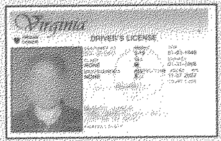
Do not accept this transcript unless the certified copy Certificate of Live Birth raised seal is affixed thereon.

ANY ALTERATION VOIDS THIS TRANSCRIPT

Counterfeit New York Birth Certificate

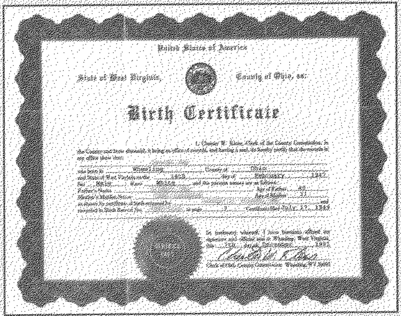
WEST VIRGINIA
DRIVER'S LICENSE

Counterfeit West Virginia Driver's License



Virginia
DRIVER'S LICENSE

Counterfeit Virginia Driver's License



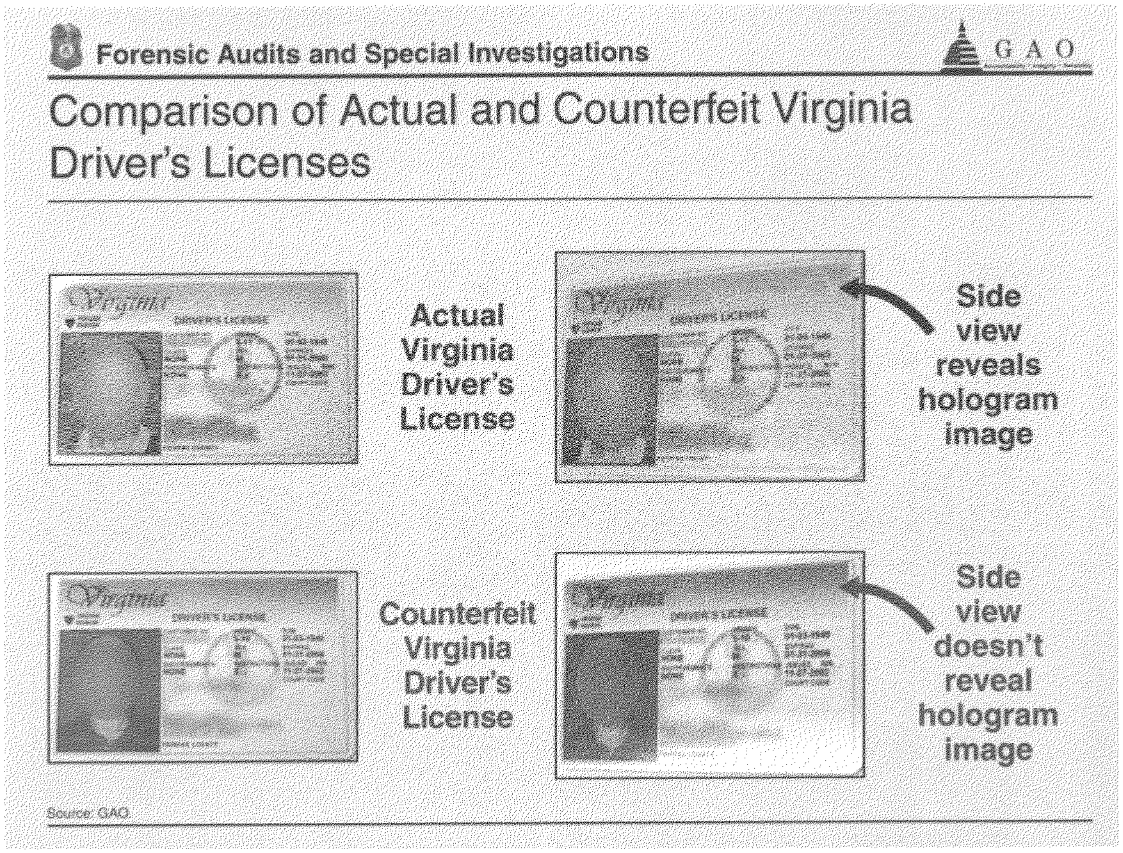
United States of America

State of West Virginia, County of Ohio, ss:

Birth Certificate

Counterfeit West Virginia Birth Certificate

Source: GAO.



Forensic Audits and Special Investigations

GAO

Comparison of Actual and Counterfeit Virginia Driver's Licenses

Actual Virginia Driver's License

Side view reveals hologram image

Counterfeit Virginia Driver's License

Side view doesn't reveal hologram image

Source: GAO

AssureTec
Systems, Inc.

Statement of R. Bruce Reeves

Wednesday August 2, 2006

United States Senate
Committee on Finance

Mr. Charles E Grassley, Chairman

Mr. Chairman and other members of the committee, good morning.

First, I wish to thank you for inviting me to give testimony regarding commercially available technologies to assist our border inspectors in detecting fraudulent documents. AssureTec Systems, Inc. Of Manchester, New Hampshire is one of the companies providing automated document authentication systems. These systems are not designed to replace human inspection, but rather, to assist the inspector in the daunting task of visually inspecting every single identity document. While it is not possible to expect a border inspector to memorize the specific security attributes designed into thousands of document types that may be presented at a border, it is very possible to program a computer to do exactly that. Border agents, no matter how much training, cannot, without automated technology, keep up with the urgent requirement and necessary resources to screen each traveler's documents for authenticity while at the same time measuring the behavior of the person presenting identity at the border.

I have been specifically asked to address three basic questions: (1) the current viability and availability of such technology, (2) examples of current implementations by governments of other nations, and (3) an estimate of the cost for adding this technology to the U.S. border management system.

Our company delivered its first commercial border product for use at the Santiago airport in Chile in February of 2004 where Unisys South America integrated our technology including an independent biometric solution into a state of the art exit/entry system for the Customs and Immigration of Chile. For the past two and a half years since its acceptance by the Police Authority of Chile, the system has operated 24/7 as a front line aide logging each entry and exit as well as screening for false or altered documents. Facial and finger biometrics and watch list comparisons were integrated as well into this solution. The solution operates behind the scenes and in a few seconds delivers an alert in the event the system detects preset levels of risk.

When alerts are encountered, the operator can click on the specific item for further detail.

A similar border management solution has been installed by Merit Technology of Melbourne, Australia for Papua New Guinea border management where again watch list checking is also integrated with our document authentication. This solution also includes a vetted passenger manifest for flights in and out of the country.

Our systems are also being used in both Thailand and Singapore in the e-passport enrollment process to assist in determining that the breeder identity documents presented are authentic.

For the past eighteen months our system has been used in the Phase III implementation of the Transportation Workers Identity Credential (TWIC) by Bearing Point in the enrollment process and our systems are currently being piloted in a major European bank and in several car rental companies.

Clearly, the technology is commercially viable and available off the shelf for deployment to U.S. borders.

Our company does not typically provide end user applications and pricing. We normally work together with systems integrators who integrate our technology to the specification of the end user, in this case border management.

The committee has advised us that there are 502 land border entry lanes in the United States. Assuming a technology cost per lane of approximately $4,000 and an annual servicing fee after the first year between of $700 and $800, the raw technology cost to assist in entry only is about $2million initially and slightly less than $400,000 annually for services after the first year. We would estimate an integrated networked border solution would run up to three times that number before integration with biometrics.

The Government Accountability Office (GAO) reports that in 2002, there were about 440 million primary inspections conducted at the 330 primary land, air and sea entry points, by 4,775 inspectors[1] of which 279 million inspections were of foreign nationals[2]. Using a three year model, assuming 80% of the estimated 440 million crossings (350 million land entries annually) are at the 502 entry lanes, the authentication technology cost per land crossing would come to less than $.003 per crossing (about $.01 estimated for the integrated solution) .

To conclude, we believe automated document authentication is both commercially viable and economical.

Thank you for inviting me to testify today and I am willing to answer any further questions the committee has of me. I will submit the balance of my written testimony to the committee for your consideration.

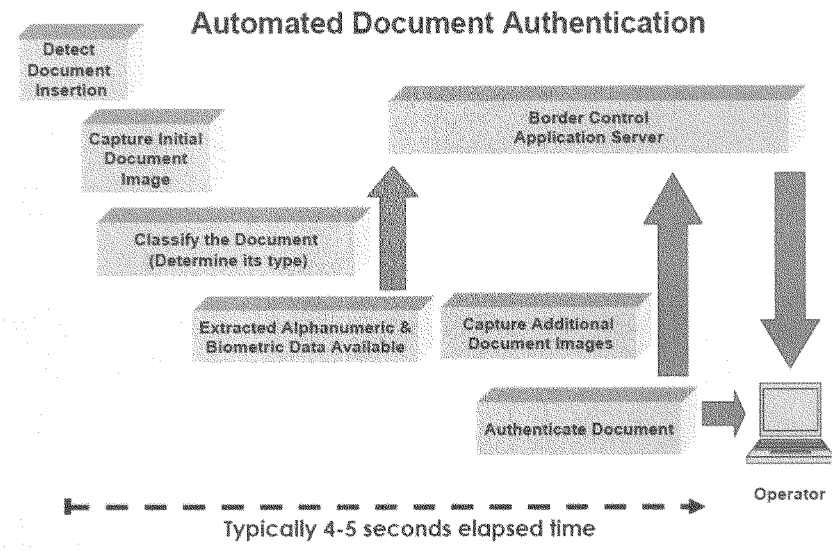
[1] "Protecting the American Homeland; A Preliminary Analysis" 2002 Pg 32 and ibid Report to Congressional Committees pg30

[2] ibid Report to Congressional Committees pg 54

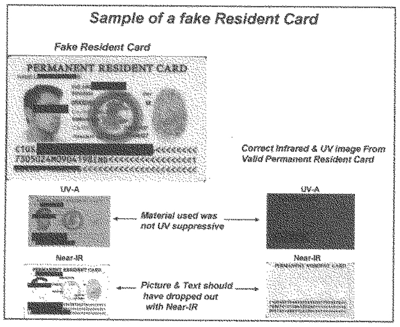
AssureTec
Systems, Inc.

How Our System Works

The following diagram is a simplified overview of how our system functions. The system captures an image of a document, identifies the type and issue of the document, and performs any number of examinations of each document using up to 5 different light sources, depending upon the specific security features and attributes of each document. The system extracts user-selected information from the document, including alphanumeric and biometric information, which can be passed in parallel to any number of specific databases/applications for such things as lost/stolen document checking, terror watch list checking, and the like. The operator is notified, typically in under 5 seconds, of each anomaly identified if any in the document.

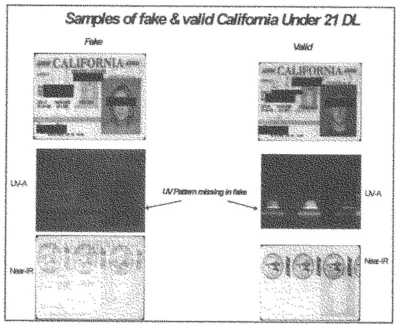

Automated Document Authentication
Detect Document Insertion
Capture Initial Document Image
Classify the Document (Determine its type)
Extracted Alphanumeric & Biometric Data Available
Capture Additional Document Images
Authenticate Document
Border Control Application Server
Operator
Typically 4-5 seconds elapsed time

Many security characteristics within a document are only visible under different light sources, such as UV-A, UV-B, IR and coaxial light, as seen in the following charts. Our system is designed to check for the presence of these attributes, and many others and notify the inspector accordingly.

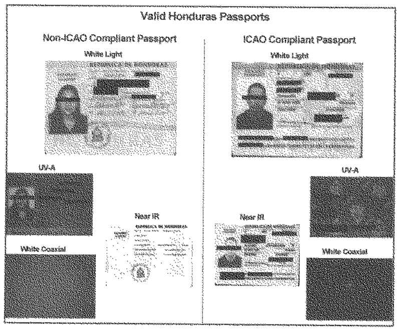


Sample of a fake Resident Card

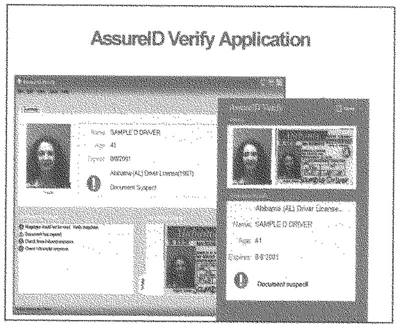
Fake Resident Card
PERMANENT RESIDENT CARD
Correct Infrared & UV image From Valid Permanent Resident Card
UV-A
UV-A
Material used was not UV suppressive
Near-IR
Near-IR
Picture & Text should have dropped out with Near-IR



Samples of fake & valid California Under 21 DL



Valid Honduras Passports



AssureID Verify Application

Name SAMPLE D DRIVER
Age 41
Expires 8/8/2001
Alabama (AL) Driver License(1997)
Document Suspect

Alabama (AL) Driver License...
Name: SAMPLE D DRIVER
Age: 41
Expires: 8-8-2001
Document suspect!

AssureTec
Systems, Inc.

The Challenge

There are many challenges to our border agents

- We estimate there are thousands of variations of ID documents in circulation worldwide at any given time.
- In North America alone there are currently 381 drivers license variations in circulation issued by the 68 states and provinces and territories
- Long lines at the borders are an unacceptable side effect of slow and careful human document screening.
- "Fake" or altered ID documents have gotten much better, more readily available, and cheaper [3]
- Post 9/11 it is critical that the information taken from the document be screened against such things as stolen document lists, and terror watch lists.

Attachments:

1) "Automated Authentication of Current Identity Documents", T. Kuklinski, 2004 IEEE Conference on Technologies for Homeland Security, Cambridge, MA, April 21-22, 2004.
(http://www.assuretec.com/content/whitepapers/Automated%20Authentication%20of%20Current%20Identity%20Documents.pdf)
2) Merit Technology Border Management System brochure, system installed in Papua New Guinea.

[3] See "*In the ID Wars, the Fakes Gain,*" Warren St. John, New York Times, nytimes.com, March 6, 2005

2004 IEEE Conference on Technologies for Homeland Security, Cambridge, MA, April 21-22, 2004

Automated Authentication of Current Identity Documents

Theodore Kuklinski, Ph.D.
Director of Research, AssureTec Systems, Inc., Manchester, NH

Abstract: *Much has been said about the difficulties in screening persons for possible identity fraud or security concerns based upon use of current driver's licenses or passports. The most often reasons given are the lack of standardization of security features and the layout for these documents. This criticism is focused on the inability of even a trained person to recognize valid documents and the specific parameters for each of these documents. In this paper, the focus is on the value of machine screening of the identity documents in circulation. The distinction is between human screening and the power of machine processing. The diversity of the identity documents and the issuer's attempts to exert their own unique identity for their documents is actually a benefit to machine screening. The rich variety of specific layout and production characteristics provide many examination points for evaluation. The processing power, storage capacity, and imaging options, only recently available at a reasonable price point, make real-time examination of all of the unique properties and a subsequent risk analysis of the results a practical approach.*

One of the most visible changes in society today is the need to present identity documents (ID's) in many more situations. A key objective in improving public security is the interdiction of individuals using counterfeit or stolen ID's to cross borders, use public transportation, open bank accounts, or enter facilities. However, security personnel are presented with an overwhelming number of identity documents and have only seconds to examine them, verify their authenticity, and approve the presenter.

New generation reader/authenticator/validator (RAV) technology can assist in the ID screening process for the wide variety of existing identity documents such as passports and drivers licenses. Such devices can read the information on the ID, authenticate the ID, and provide a security risk analysis. Acting as an inspector's automated assistant, their use permits an inspector to focus on evaluating the behavior of the presenter while the reader handles the detailed analysis of the document. A much more thorough ID inspection is possible, checking for many more security features, some of which are not accessible to the inspector without special equipment. More ID presenters can be processed faster with fewer inspectors at lower overall cost and with higher security confidence.

Almost 100,000 fraudulent documents were intercepted at U.S. ports of entry in 1998 [1]. How many are not being intercepted? The technology to create reasonable forgeries of current identity documents is both affordable and available. There are still many older style, unexpired, laminated licenses (e.g. New Jersey) in circulation; forging them requires little more than an inexpensive scanner, printer and laminator. Equipment capable of printing on the plastic card stock used for most ID cards today is now well within the budget of the average personal computer user. There are a variety of publications [2, 3] and websites that describe techniques for creating false identity documents. Other sources, rather than facilitating getting a counterfeit document, provide official looking secondary ID's that give the impression that they *could* be official documents, complete with genuine looking security features. They rely on the fact that document inspectors are not familiar enough with valid issued documents to recognize the bogus ones.

In the US, there have been calls for a national identity card with the idea that standardization of layout and security features will lead to better security; a standardized card would be easier to authenticate by the average inspector. Likewise, the perceived difficulty of validating current issue documents has spawned a movement toward greater use of biometrics in conjunction with ID's. While this is a worthy goal, it requires the step of enrollment to collect the biometric information. It will likely be a long time before currently issued documents are expired and replaced by "more secure" biometric documents. There has been a request [4] to push off the deadline for biometric passports from "visa waiver" countries until 2006.

In recent years, there has been a definite trend toward more secure identity documents, particularly driver's licenses. American states and Canadian provinces have largely converted over to more secure ID's incorporating such security features as ghost photos, check digits, security laminates, holograms, micro-printing, or patterns visible only in ultraviolet (UV), near-infrared (IR), or retro-reflective light and biometric features, magnetic stripes and barcodes. This trend also applies to passports and visas, which for many years have had a machine readable zone (MRZ) and a somewhat standardized layout for photos and other information.

The American Association of Motor Vehicle Administrators (AAMVA) organization provides standards for DL/ID (Driver's License/Identification) cards [5] and makes recommendations for placement of information on the card and the use of security features. Even within these guidelines, ID's issued by different states vary greatly in appearance. AAMVA admits "The increased use of the card for purposes other than proof of the privilege to drive have greatly increased the motivation to alter or counterfeit the DL/ID card." There is the desire, just as with state license plates, to impart some distinctive local identity. Sometimes license documents are not necessarily designed with readability in mind, for either the human inspector or machine readers, or in a manner that takes most advantage of the security features that may be available.

On the passport and visa front, the International Civil Aviation Organization (ICAO) has issued standards [6] for passports, visas, and other ID cards. For some 20 years, the ICAO has recommended the use of Machine Readable Zones (MRZ's), printed using the OCR-B font, in order to facilitate machine reading of such documents and as many as 300 million machine readable travel documents have been issued based on MRZ's. ICAO has established standards for the other areas of documents such as passports but there is still a large amount of discretion available to governments for customization of a unique appearance and the use of individual security features. Nonetheless, many passports and visas are non-standard or not machine readable (many even handprinted), and these will be circulating for years.

Screeners may become adept at recognizing the most common variants, but it is unreasonable to expect that security personnel or gate agents can memorize the detailed features found on the thousands of types of ID's presented for verification. Subtle design changes or even entirely new document designs are issued frequently. It is difficult for the inspector to keep up with these changes. Asa Hutchinson, Under Secretary for Border and Transportation Security at the Department of Homeland Security (DHS), in testimony before the U.S. Congress [7], acknowledges the problem: "there are more than 240 different types of valid driver's licenses issued within the United States" and further admits that "it would not be easy for CBP inspectors to have a passing familiarity with, let alone a working knowledge of, each of these documents. " Consider driver's licenses in the U.S. In addition to the standard issue driver's license and its older issue unexpired version, there are non driver ID's, Commercial, Provisional, Temporary, Under 21, Moped, Boat, and a host of other variants. Maryland, for example, has over 20 old and new license variants, with many of the variations printed in different colors.

So it remains that, for each document presented, an inspector must quickly know which visible security features to check and must instantly know where to look on a document to pull out necessary information such as the expiration date. There is no uniform date format for driver's licenses which is important in age verification situations. Most existing documents contain the same basic types of information. Unfortunately, the locations and format of such information varies widely with document type. The inspector must decode this information efficiently, reading small print in often poor and variable lighting conditions. They also need to be able to compare the photo on the ID and the face of the presenter or perhaps match the name on the ID and an airline ticket.

What aids are available to the person inspecting ID's to assist them in recognizing the wide variety of ID's that may be presented to them? Manuals [8] are available to law enforcement agencies and businesses, such as those serving alcohol, for the purpose of checking U.S. and Canadian driver's licenses. Issued annually, these so called "bar guides" commonly display examples of the current and unexpired past issue licenses and list some common features to check. They may not contain many of the license variants that exist, particularly "Under 21" licenses, which are issued in a vertical format by many states.

While such guides may indicate that there should be a UV pattern, there is no indication of what that pattern is. How likely is the inspector to hold up a long line while they consult reference material to validate their fuzzy memory of some document feature? Equivalent services in the form of publications, software, and web reference sites, are available for passport and other international documents. Such resources draw a fine line between providing enough information for someone to validate a document, but not such complete information that a forger could produce a very good fake ID from the information provided.

We have seen the burdens that are put on document inspectors. Could a machine reader provide some assistance in this critical task? Machine readers have been available for some time that can read passports and other ID's that have MRZ's. Future identity documents will likely be equipped with many more features to make machine reading of them more efficient. We already are seeing the growth of smart card technology in ID's and magnetic stripes and barcode have been available for some time already. Nonetheless there are still a great number of "legacy" ID's that it would be useful and economically desirable to read.

Machine readers amplify the inspection ability of inspectors by providing automatic eyes on aspects of the presented ID they would be hard pressed to get otherwise. There may be a tremendous variability in the experience level of inspectors. They are subject to the many external factors – distraction, inattention, boredom, and even bribery. With the quality level of fraudulent ID's so high, the cursory glance of even experienced inspectors may easily fail to pick up the minor variations that could be telltale signs of document fraud. In most human inspections, typically an easily performed UV check is not performed. Machine readers don't get tired and can check all relevant details automatically and quickly. A machine reader can alert the human check to precisely those aspects of the document that may require closer inspection by providing a risk score. Their use can be an adjunct to the human inspection process, freeing them to focus on the behavior aspects of the presenter. In many checking situations, the focus is actually on the task of insuring that the face on the document matches that of the live person, given the vagaries of hairstyle, glasses, or facial jewelry.

A new generation of reader devices is available now, capable of fast full page color reading of passports and other identity documents. They feature automatic document sensing of up to passport sized documents (including driver's licenses), imaging in visible, IR, UV, and other lighting conditions, are trainable, and capable of scanning, reading, and authenticating in a few seconds. A modern reader system typically consists of a video camera, controllable lighting system, and a processing unit. The processing power, storage capacity, and imaging options, only recently available at a reasonable price point, make real-time examination of all of the unique properties and a subsequent risk analysis of the results a practical approach. Document validation can be performed in a few seconds, an important factor where there may be long lines of people to be processed in a short time.

The diversity of identity documents and issuer's attempts to exert their own unique identity for their documents is actually a benefit to machine screening. The rich variety of specific layout and production characteristics provide many examination points for evaluation. An ID can easily be analyzed in a top-down fashion. Once the specific type of ID and particular issue are known, then one can look to a knowledge base of specific examination features that can be associated with that document. The position of particular fields may vary between issues. Certain unusual fonts may be used. Micro-printed areas are present in some modern licenses and can be highlighted. Under UV lighting, there is often a visible colored pattern or repeating pattern. In order to make it easier for machine reading of information, important text fields may be printed in ink which will be IR visible, allowing the scenic background information on many ID's to "drop out".

For speed of analysis, CCD color cameras can be used to capture the image. Real time video capture is feasible with the use of IEEE 1394 or USB-2 interface connections. This has the advantage of no moving parts, unlike scanners where either the document or reading head moves, requiring significantly more time for image capture. In the same time period, a camera based system can take several pictures of the document, each at different exposure settings and under different lighting conditions.

Older passport readers needed to capture only a portion of the document, typically just the MRZ. Now an entire passport page can be imaged in full color at sufficient resolution to enable accurate OCR of information fields, and even for reading barcodes. Cross checking of data derived from the MRZ and the data in the non MRZ region is possible. One of the driving forces toward full page reading is that it allows the automatic extraction of the photo which is important for matching against the live subject or checking against watchlists. With a full page document read, the image can be immediately displayed to the inspector. There need be very little time lost in the throughput process since the inspector could immediately inspect the color image of the document just as they might view the physical document. Smaller sized documents, such as driver's licenses, can be captured with the same system.

Older MRZ readers needed to capture only a binary image for OCR purposes. Earlier full page readers worked with gray scale images which didn't require as much processing power. However, color information is important for authenticating today's ID's. There is much information in a color image that can be used to identify the type and issue of an ID, and for analyzing various security features (e.g. multicolored UV patterns). Color filtering and image processing can be performed to enhance any of the information fields for OCR or other purposes.

Modern ID's usually contain security features that require the document to be illuminated under a number of different lighting conditions. Camera based readers make the task of utilizing multiple lighting sources in a short time feasible. They may use uniform white light for the capture of the visible image, near Infrared (B900) light for reading carbon based inks and security features without the color background, ultraviolet (UV) for detecting overlay patterns printed in UV sensitive inks, retro-reflective light for reading special laminates, and other specialized lighting for such features as holograms. With camera based systems, it is a matter of capturing an image frame under each of the lighting conditions, setting the exposure and gain, and switching the lights. Calibration techniques can be used to compensate for uneven lighting to generate a uniformly lit image, equivalent to a scanner image.

Older readers, which only had to deal with reading the single OCRB font found in MRZ's, could be ROM based peripheral devices with limited memory and processing power which communicated by RS-232 interface. Today, readers based on a dedicated PC architecture have the advantage of being able to be quickly upgraded with software enhancements, upgraded with faster processing power, vastly superior communication options, and larger memory space which allows processing of multiple high resolution color images.

Due to the fact that the entire field of view can be monitored continuously, the video image feed can itself be used as a sensor to detect when an ID has been inserted in the reader. Upon detection, the image can be located, deskewed and cropped to contain just the ID image. This image can be compared quickly against a knowledge base of known document types. The type of document can be verified by checking for the presence of certain known distinctive features. Given a known document type, then additional images under appropriate lighting conditions can be captured and the layout for that particular document can be obtained from the knowledge base.

Extraction is the process of deriving usable information or images from the document fields. A given area may have very field specific image processing operations applied, such as contrast enhancement, color filtering, dilation/erosion, sharpening, or others. In some cases, this is to enhance images before applying OCR processing to fields such as MRZ's, ID number, Name, Birth Date, or Expiration Date. In many cases, text information is available in the IR image with the colored scenic background dropping out. Using appropriate OCR engines, even passport punched text or non Roman alphabets, can still be read. OCR results can be post- processed, for instance to create a uniform format for dates or perhaps to calculate current age from the birth date. Likewise, barcode images can be decoded from the image itself if the resolution is sufficient.

One of the most useful features of a reader/authenticator system is the ability to recognize arbitrary patterns that may occur in documents. One use of this ability is to test for the presence of certain sometimes subtle features which are markers for different issues of a given document. Another is for the verification that specialized patterns used for security purposes are present. Multicolored UV patterns are now being commonly used. Sometimes breaks in the patterns may indicate tampering. These types of authentications are critical in today's environment. While a forged document may look almost perfect to the eye, getting all the document elements correctly in all lighting conditions is more difficult to achieve for forgers.

A large library of authentication tests can be developed and used. These tests can be tailored to the types of forgeries or modifications likely to be done a particular type of ID. An authentication test is possible for any of the security features present in a given document. There can be general tests for the presence of certain colors or ink sensitivity in various lighting conditions, for instance to see if there is an IR component to ink or a strong UV component where there should not be. Cross checking between different exemplars of the same information, e.g. the birth date derived from the MRZ and that displayed elsewhere on the passport can be used for authentication. With the ability to decode the barcodes, magnetic stripes, or smart chip info, comparison can easily be made between information derived from these features and those derived by OCR extraction of the text information from the corresponding human readable fields. On passports, the MRZ information is easily compared with information from the upper portion of the document. Certainly, any information garnered from text reading such as name or ID number could be used to query an external data base to verify the validity of the document's other information. Such an inquiry could also return a stored photo or other biometric. More discussion of the various types of security features can be found [5, 9].

The importance of any authentication checks can be weighted. They can be consolidated to arrive at a risk score for a particular ID presenter. The risk can be weighed against the entitlement that presenting the card allows. An automated reader system provides an audit trail of document inspection. Images captured from the process can easily be stored or forwarded for more detailed analysis, not necessarily by the frontline inspector. A networked system could funnel any risk cases for a secondary inspection. In many situations, there are other opportunities to apprehend the presenter of a false ID, e.g. in the case of airport screening, before boarding the plane or even upon disembarking at the destination.

One of the most critical components of an automated authentication system is its knowledge base of document characteristics. It must be secure and encrypted to prevent potential forgers from using this information. By use of an encrypted knowledge base, even the inspectors, who may potentially be subject to compromise, may not be privy to security features that are being used in the authentication process. The knowledge base must be capable of being frequently updated as new documents and variations are issued. Being able to easily train the knowledge base for new documents is an important component. It must be flexible and expandable in its ability to deal with new security features that may be added. It must be adaptable and programmable in terms of the risk incurred by a given security feature alert (which could be due to dirt or wear). The knowledge base is maintained through cooperative arrangements with government agencies and other access to known good and falsified documents.

Inspectors are presented with a tremendous variety of ID's and have a difficult time authenticating them and keeping up to date with what constitutes a valid document. A new generation of reader/authenticators can help automate the ID inspection process for existing travel documents. These devices are useful in detecting totally forged documents, modifications to otherwise valid documents, and flagging the use of valid ID's by different presenters. Use of these new units minimizes the dependency on the inspector's document expertise, helps them be more efficient, and provides a greater degree of security.

References

[1] James Hesse, "Counterfeiting and Misuse of the Social Security Card and State and Local Identity Documents," Testimony before U.S. House Judiciary Committee, Subcommittee on Immigration and Claims, July 22, 1999.

[2] Max Forge, How to Make Driver's Licenses and Other ID on Your Home Computer, Loompanics Unlimited, Port Townsend, Washington, 1999.

[3] Sheldon Charrett, Secrets of a Back Alley ID Man: Fake ID Construction Techniques of the Underground, Paladin Press, Boulder, Colorado, 2001.

[4] Gary Thomas, "Bush Administration Asks for Extension of High Tech Passport Deadline," Voice of America News, March 24, 2004.

[5] American Association of Motor Vehicle Administrators (AAMVA), Personal Identification – AAMVA International Specification – DL/ID Card Design, September 25, 2003.

[6] International Civil Aviation Organization (ICAO), Document 9303, Machine Readable Travel Documents, Part 1 — Machine Readable Passports (2002), Part 2 — Machine Readable Visas (1994), Part 3 — Size 1 and Size 2 Machine Readable Official Travel Documents (2002), ICAO, Montreal, Quebec, Canada.

[7] Asa Hutchinson (Under Secretary DHS), Testimony before U.S. Senate Committee on Finance, September 9, 2003,

[8] Drivers License Guide Company, ID Checking Guide, 2004 Edition, Redwood City, CA, 2004.

[9] Bruce Monk, "Designing Identity Documents for Automated Screening", 2004 IEEE Conference on Technologies for Homeland Security, Cambridge, MA, April 21-22, 2004.

Merit BMS

Border Management System

In an age where international travel is common and border traffic is constantly increasing, so do the risks and threats associated with terrorism and organised crime. The *Merit Border Management Solution* (BMS) provides the essential components necessary to effectively manage all aspects of immigration and border control at all entry points.

The system is characterised by high accessibility, quick response times, and full functionality in extreme load situations - all without compromising the quality and safety of border control. Merit BMS is comprised of the following key functions:

Passports

The Tardis Passport System (Travel and Related Document Issuance System) is the passport and travel document issuing component of Merit BMS. It is used to support each step in the passport process from receiving an application through to data entry, research, authorisation, printing and quality control. It manages document stock control and provides reports and statistics on system usage so that office efficiency and productivity can be monitored and managed.

Visas & Permits

Similar to the passport system, the Merit Visa & Permit module is used to support each step in the visa or permit process, including payment receipt and lodgement of applications, data entry, research, authorisation, sponsorship management, printing and quality control. The module can be centrally administered to provide remote access to overseas posts, and provides reports and statistics on system usage.

Border Management

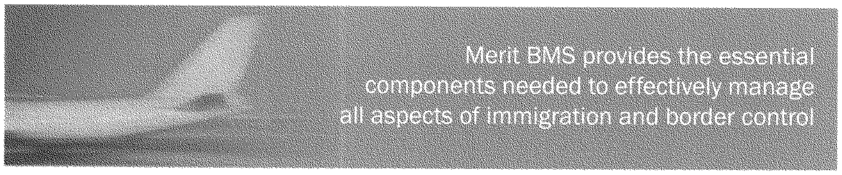
The Border Management component of Merit BMS comprises several functions including: Immigration Policy, Flight Management and Passenger Movement modules.

The Merit BMS Immigration Policy Engine manages the rules associated with the movement of passengers and can be tailored and aligned with countries' specific immigration legislation and policies. On processing an arrival or departure, Immigration Policy rules are applied against passenger movements. Rules include alert checking, reconciliation against Advanced Passenger Information from airlines, unbalanced passenger movement, high-risk countries, visas and permit verification, and crew, transit and visitor policies.

Passenger movement management is the primary function of any border management solution. In conjunction with the Immigration Policy Engine, Merit BMS rigorously reviews each movement for document authenticity, movement alert hits, movement inconsistencies, and permit and visa holdings, along with any other rules required by immigration departments to ensure passengers are thoroughly screened at the border. Throughout the process, the Primary Line Officer is kept informed of any issues and can escalate the movement to a superior officer for secondary inspection at any stage in the process.

Advanced Passenger Information

The Flight Management module of Merit BMS facilitates the entry of Advanced Passenger Information (API) prior to a flight arriving for immigration clearance, enabling pre-screening of passengers against the Movement Alert List, and ensuring accurate reconciliation of expected passengers against actual movements processed by Immigration.


Merit BMS provides the essential
components needed to effectively manage
all aspects of immigration and border control

MERIT

Movement Alert List

The Movement Alert List of Merit BMS stores details about travel documents and people of concern to immigration departments and related law enforcement agencies such as Justice, Police and Customs authorities. The system facilitates various levels of movement alerts and security access restrictions, including overt and covert alerts, and provides tools for maintaining movement alerts and monitoring movement alert activity.

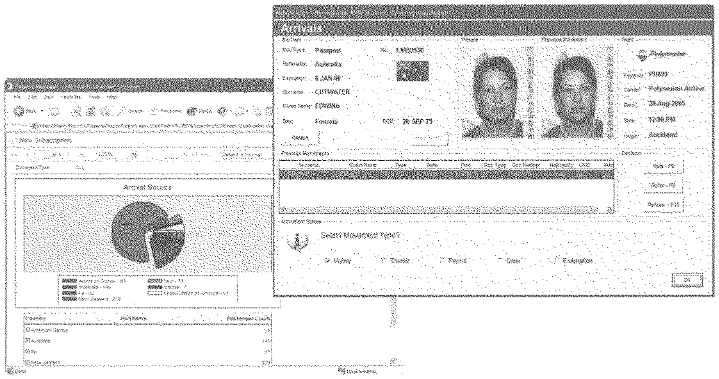
Reports and Enquiries

The powerful features of Merit BMS are complemented by a suite of effective and informative reports and enquiries. It is critical that immigration departments, along with the agencies they work with, have insight into immigration and border activity, whether it be alert activity, movement history, travel document issues, over-staying visitors, or demographic information. Merit BMS provides the tools to quickly access relevant information.

A Fully Integrated Solution

Merit BMS can tightly integrate with existing immigration systems to complement the border management process. Critical data associated with monitoring and managing border movement may be maintained in existing systems, and Merit BMS can seamlessly integrate to these sources for validating immigration policy rules and processes.

In addition, Merit BMS interfaces to numerous document authentication solutions, highlighting the system's independence from other technology. The system currently supports the *i*-Dentify reader-authenticator from AssureTec Solutions, and can be enhanced to operate with a client's existing technology, as well as future biometric document technology, to ensure the system will be a solution for the future.



Arrivals

Doc Type: Passport

Nationality: Australia

Surname: CUTWATER

Given Name: EDWINA

Sex: Female

DOB: 20 SEP 75

Carrier: Polynesian Airlines

Date: 28-Aug-2005

Time: 12:00 PM

Origin: Auckland

Select Movement Type?

Visitor Transit Permit Crew Exemption

USA
Merit Technology, Inc.
695 S.Nardo Ave G.5
Solana Beach
CA 92075

Phone: +1 888 637 4838
Fax: +1 858 630 2036
Email: info@merittech.us
http://www.merittech.us

Australia
Merit Technology Pty Ltd
ABN 78 074 588 668
18 Stirling Crs
Surrey Hills, VIC 3127

Phone: +61 3 9830 5566
Fax: +61 3 9830 1764
Email: info@merit.com.au
http://www.merit.com.au

AssureTec
Systems, Inc.

Friday, August 11, 2006

Senate Finance Committee Hearing "Border Insecurity, Take Two: Fake IDs Foil the First Line of Defense." August 2, 2006
Supplemental Statement of R. Bruce Reeves (Panel II)

Attention: Bob Merulla
Editorial and Documents Section
United States Senate
Committee on Finance
Room SD-219
Dirksen Office Building
Washington, DC 20510-6200

Dear Mr. Merulla;

This supplemental written testimony is submitted in response to the Chairman's closing remarks regarding further clarifications and new questions remaining open until today. While preparing these supplemental remarks, the London terrorist events prompted even more significant and important observations which I have addressed as well in light of the heightened alert levels and the original intent of this hearing.

General Questions and comments:

1. Mr. Ahearn of CBP testified that the strategy for CBP was to wait until the WHTI was implemented because the CPB agents were not able to handle the "240 unique drivers license types used every day in North America to cross our borders."
    a. First, WHTI is a very controversial and expensive initiative and may never be implemented in its current form. To risk our borders every day for at least another two years, and perhaps longer, waiting for the initiative to become effective, appears flawed. In many respects WHTI is redundant with the goals set forth in the REAL ID Act, but, unlike REAL ID, it does not address correction of the issues necessary to establish true identity. REAL ID is flawed and needs adjustment, but even in its current form, it represents a more viable approach for a secure border crossing document and has broader implications in combating the more general issue of identity fraud. The use of a biometric link for entry/exit is easily implemented by transparently capturing such on entry and exit.
    b. Even if WHTI is ultimately implemented, there is still the issue of the transition period where both existing and "a new smart document" will be in circulation. This is likely to be several years due to infrastructure limitations for enrollment. Also, there is a question as to what the "fall back" position will be in the case of lost, stolen, or damaged

documents. Our product already reads and authenticates approximately 550 types of government-issued North American identity documents (it is regularly increasing). We also support 100% of the ICAO-compatible passports now required for entering the U.S. and more than 350 variations of passports from more than 150 countries. This represents 98+% of all passports. About 30% of these types of documents are not ICAO standard. WHTI will have no impact on CBP agents' ability to recognize and authenticate these documents. Nor will it aid in overcoming the human factors such as fatigue, bribery, distraction, extortion, and job dissatisfaction or the aforementioned failure modes for a "smart" ID.

2. Beyond borders, the infrastructure of the United States is exposed daily to the millions of false documents in circulation. To rely on comparison against "no fly" lists and criminal/terrorist watch lists without vetting true identity assumes that we know all of the "bad guys" and this is obviously absurd. Now, while we are under the highest alert possible for international flights, Papua New Guinea has a more secure electronic manifest to check for terrorists than does the United States. Migrating automatic document logging and validation to domestic airline and critical infrastructure is only logical. What good is a non-vetted "no fly" list? Anonymous screening can be applied privately and securely until an alert is experienced much like current cell phone records are maintained.

3. Clearly, the technology discussed and demonstrated during the second panel of this important hearing **can only add value to the security of our border management process**. This is true today with the myriad identity documents used in border crossing, and it will remain true even if/when the utopian world of CPB exists with a single standard "smart" travel credential.

Comments specific to questions raised by Chairman Grassley

1. *Chairman Grassley: We heard from the Government Accountability Office that CBP failed to run name checks on their investigators and don't really have time to run name checks on every person crossing the border. Would anyone like to explain how technologies like these could help CBP run name checks more often and more efficiently?*

   It was mentioned several times by CBP during the Hearing that "standard" documents which are "machine-readable" are necessary for the CBP personnel to be able to authenticate the documents and read the information for "name checks" and document authentication.

   As demonstrated at the hearing, the technology exists to read virtually all current travel documents (passports, ID cards, driver's licenses, etc) with accuracy sufficient for parallel checks against multiple name lists, terror watch lists, known/wanted criminal lists, etc. The complete examination can overlap the inspector's normal activities and takes typically less than 5 seconds. It is not necessary to have a document with a machine readable zone (MRZ), 2D barcode, or "smart" chip in order to extract the data. Moreover, the catastrophic nature of the failure mode for "smart" chips and damage to barcodes or magnetic stripes, either caused by normal wear and tear or by deliberate destruction, makes it prudent to require the deployment of such OCR technology as a fall-back for such failures (Note: destruction of the functionality of a "smart" chip is easy to achieve and not detectable without sophisticated equipment and destruction of the document.)

As for human visual authentication of the document, standardization of documents actually makes the task of the forger easier by providing a single target to focus upon to simulate the "look and feel" of a real document. This increases the value proposition for the criminal/terrorist's effort and makes it a worthwhile investment. Because the current authentication approach relies upon checks against databases of known offenders or lost/stolen documents, stolen and fake identities are not readily detected.

Clearly better documents with improved security features and better biometrics will improve security. However, this is only true if automated tools exist at the points of entry to verify them in real-time. Human inspection often fails even on easily recognized security features due to normal human shortcomings such as susceptibility to fatigue, distraction, bribery, extortion, etc. It seems logical to deploy technology that aids inspection of documents that are currently in use and will read/authenticate new generations of documents as they become available.

2. *Chairman Grassley: Ms. Kephart's prepared testimony discussed the possibility of using real time lost and stolen passport data from Interpol and using that at border checkpoints. So, I'm wondering if this technology could work with that information. Can anyone explain whether it'd be possible, just as an example, to automatically read passports with these kinds of scanners, even if the passports were not originally designed to be machine readable, and then check their numbers against a list of known lost or stolen passport numbers?*

As pointed out at the hearing, at a minimum, there needs to be a link from the front-line inspection station to the database of lost/stolen documents. The current Inter Agency Border Inspection System (IBIS) currently provides some of this functionality. However, if there is a failure to scan the MRZ, then only minimal data is entered and there is no passport number check performed. If such a link were enabled, then all travel documents could be checked whether there was damage to the MRZ, "smart" chip, or barcode. Even documents that were not designed for machine readability can be read and checked automatically. The technology demonstrated reads the information on the document and extracts the photo whether or not it was designed for machine-readability. If it has machine-readable features then that data is read and automatically compared to all redundant sources of data on the document.

Until very recently, the US and most countries all issued some non-machine readable passports. This was generally the case for passports issued at embassies around the world. The current VISA-Waiver countries also issued many non-machine readable documents. These countries were required to start issuing machine-readable documents in October of 2005; however, documents issued prior to that date will be good for the next 8-9 years. Even with the Western Hemisphere initiative, it is questionable that the enrollment and vetting of all persons wishing to cross our borders can be done with any degree of security prior to the end of 2008.

It is important to note that enrollment for a new more secure document (ePassport, "smart" card, etc.) requires close examination of an applicant to determine if the identity being used to get this new credential is real and if it belongs to the applicant. This process relies very heavily upon examination of existing documents and extraction of data thereon. The enrollment process for the new travel credential needs to be similar to what was envisioned in the REAL ID Act for U.S. drivers license enrollment. All breeder documents must be vetted, otherwise a secure, legitimate travel credential could be issued based upon fraudulent documents being presented.

The current US VISIT program is a good example of a case where very little document examination takes place. The data extracted from the passport/visa is checked against a watch list and the fingerprint is checked (sometimes). There is no checking to ensure that the document presented is real, the identity is real, or if it belongs to the individual. The State Department database of VISA information, such as photo/fingerprint, is not generally available to the front-line inspection station for verification. For the purported US Citizen, Resident Alien, or VISA-Waiver member entering the country, there is virtually no checking to ensure that the identity is real and not stolen from someone else.

This data is then "sealed" with biometric data. The biometric is useful to verify if and when that person exits the country (provided they do not use an assumed US identity). It does not inhibit an undesirable from remaining in the country and assuming another identity.

Virtually all fraudulent documents are detected by CBP in secondary inspection due to suspicious behavior detected by an alert inspector. The number of fraudulent/altered documents seized in the past year was set at 84,000 by Mr. Ahern. This is more than 40% lower than the number seized prior to the merger that formed the DHS. There is very little training and there are minimal tools devoted to fraudulent document detection. Government sources close to the process have estimated that for every fraudulent/altered document seized there are nine that are not detected. The GAO test would suggest that this might be a low estimate.

Moreover, visible covert security features built in to the US Passport and VISA cannot be taught to our 5000 frontline inspectors for fear of compromising them. Nor can specific indicators on documents, such as those carried by some of the 9/11 terrorists be shared for the same reason. In both cases, the technology would allow for inspection of the documents for such parameters and the generation of alerts without the need to tell anyone how the examination was performed.

Finally, specific characteristics of a document can be used to alert authorities for tracking purposes where it is more beneficial to monitor the activities of the person rather than to intercept them.

AssureTec
Systems, Inc.

Please add this supplemental statement to my testimony of record which is attached to this supplemental statement.

Very sincerely,

R. Bruce Reeves

Attached Statement of Bruce Reeves originally filed with the Committee.

Testimony
C. David Shepherd
Before
Senate Finance Committee
August 2, 2006

Chairman Grassley, distinguished members of the United States Senate, Committee on Finance, ladies and gentleman, thank you for the opportunity to testify before this very important committee concerning border security.

Currently I am the Co-Chairman of the Gaming Resorts Sub-council for the Commercial Facilities Sector Coordinating Council (CFSCC), a member of the Partnership for Critical Infrastructure Security (PCIS), a member of the Real Estate Roundtable Terrorism Task Force and a member of the Las Vegas Security Chief's Association. In each of these capacities I represent only a small portion of the private sector and am honored to be a participant.

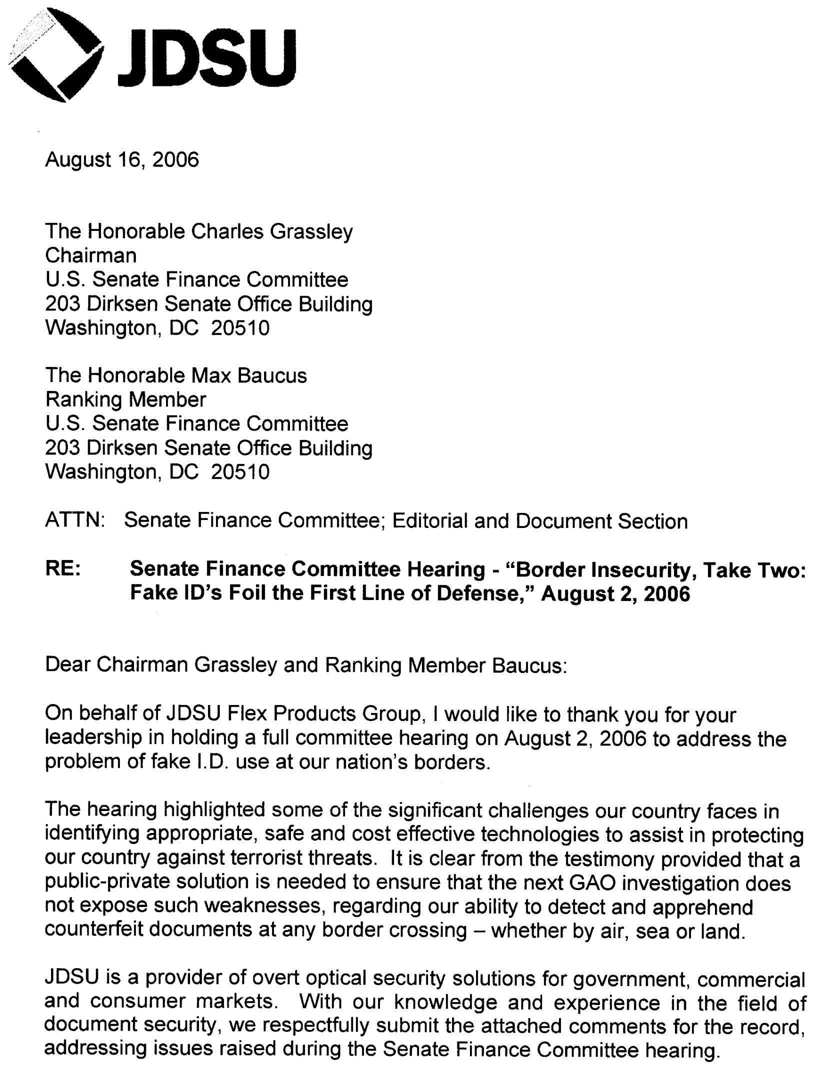
In the private sector the identification of customers, employees and business partners are important in protecting the property from criminals, terrorists and from individuals who attempt to bypass existing laws and regulations. Because of the possibility of misidentification of those who could do harm to individuals or a business; financial reporting requirements, Securities Exchange Commission, Office of Foreign Assets Control, Sarbanes-Oxley, and Gaming Control Regulations were enacted by those agencies with foresight in protecting the American way of life as a portion of each focuses upon the identification of individuals, regardless if that threat is from within or outside the companies boundaries. Each private sector business has an obligation to its employees, guests and the community at large to know the identity of individuals who interact with a company, as many private sector partners are the cornerstone of an entire community. Thus, safety is the underlying common element for proper identification recognition, not the potential for fines or business restrictions if noncompliance is uncovered by regulatory agencies.

Regardless if a fake driver's license is used by a seemingly innocent underage individual attempting to gamble in a casino or entering a nightclub, that same fake driver's license in the hands of a criminal could have a significant financial impact on a property through fraudulent financial transactions in the forms of extending credit, application for a loan or credit card purchases. However, in the hands of a terrorist the catastrophic events of 911 or London train bombings could be repeated within our borders. The fake identification is a means to an end and the choice of that end is its possessor. Las Vegas has already seen the face of terrorism, as eight of the deadly hijackers visited my city prior to September 11, 2001. Unfortunately, they were never detected by any identification system in place at that time.

Speed and accuracy in recognizing false identification are important elements in the system of protection for a business. Determining if a person is over twenty-one before he or she is served an alcoholic beverage, if the individual is actually John Doe before extending a line of credit or even offering a position within the company for a seemingly qualified applicant, cannot be left to chance or to an individuals discretion. Unfortunately, there are over ten (10) million cases of identity theft in the United States and the internet provides instruction to create false identifications. Technology has been used by the criminal element to replicate fake identification regardless of the state or country of origin, thus technology should be employed to keep ahead of those who attempt to circumvent the system.

I have had an opportunity to review various technologies and systems currently available within the private sector, which offer full or partial solutions to security and regulatory challenges under financial, criminal, civil, risk management and terrorism concerns. In the Commercial Facilities Sector many private partners have deployed systems to identify fake driver's licenses, passports and visas offered as proof of identification. I have brought one of those systems for demonstration purposes today. In addition to this system there are other systems available that primarily focus upon driver's licenses or credit cards without referring to reference manuals and without unduly inconveniencing those individuals who are being screened. Thank you Chairman Grassley and members of the Senate Finance Committee for you attention and understanding.

COMMUNICATIONS



JDSU

August 16, 2006

The Honorable Charles Grassley
Chairman
U.S. Senate Finance Committee
203 Dirksen Senate Office Building
Washington, DC 20510

The Honorable Max Baucus
Ranking Member
U.S. Senate Finance Committee
203 Dirksen Senate Office Building
Washington, DC 20510

ATTN: Senate Finance Committee; Editorial and Document Section

RE: Senate Finance Committee Hearing - "Border Insecurity, Take Two: Fake ID's Foil the First Line of Defense," August 2, 2006

Dear Chairman Grassley and Ranking Member Baucus:

On behalf of JDSU Flex Products Group, I would like to thank you for your leadership in holding a full committee hearing on August 2, 2006 to address the problem of fake I.D. use at our nation's borders.

The hearing highlighted some of the significant challenges our country faces in identifying appropriate, safe and cost effective technologies to assist in protecting our country against terrorist threats. It is clear from the testimony provided that a public-private solution is needed to ensure that the next GAO investigation does not expose such weaknesses, regarding our ability to detect and apprehend counterfeit documents at any border crossing – whether by air, sea or land.

JDSU is a provider of overt optical security solutions for government, commercial and consumer markets. With our knowledge and experience in the field of document security, we respectfully submit the attached comments for the record, addressing issues raised during the Senate Finance Committee hearing.

We would be pleased to answer any questions or provide additional information to you and the committee as you continue to oversee implementation of the Western Hemisphere Travel Initiative, Real I.D. Act and other government card security programs currently under consideration.

Please contact me at 571-276-3930 if JDSU-Flex can provide additional information or offer any assistance.

Sincerely,

Garth Zambory
Product Line Manager – Secure Documents
JDSU-Flex Products Group
430 N. McCarthy Blvd.
Milpitas, CA 95035

JDSU

Comments for the Record
U.S. Senate Committee on Finance
Hearing – August 2, 2006
"Border Insecurity, Take Two: Fake ID's Foil the First Line of Defense"

JDSU Flex Products Group Overview

JDSU is a worldwide leading provider of broadband test, measurement solutions and optical security products for government, commercial and consumer markets.

JDSU-Flex's overt color shifting ink technology is utilized as an authentication product in U.S. currency and the currencies of nearly 100 countries worldwide (80% of the value of currency in circulation today) and used as part of a layered security solution to protect against counterfeiting technologies and products including identification cards, e-passports, visas, credit cards and postage stamps. Color shifting technology is also used by 7 of the top 20 global R&D-based pharmaceutical companies to protect 25 brands of drugs.

JDSU-Flex offers such products as inks, security labels, tamper-evident labels, seals and tapes. Color shifting technology can also be applied to barcodes and incorporated with RFID technology.

The Need for Layered Security

As the Departments of State and Homeland Security seek to identify the best technology that can be used to increase security at the U.S. borders by validating identity and citizenship, it is recommended that such standards include layered, visual security protections that can seek to further protect and authenticate an electronically readable or biometric-based card. Layered security technologies should include a combination of overt, covert and forensic features and devices.

The inclusion of multiple features reduces the opportunity to counterfeit or falsify a document, and layering such technologies as RFID or biometrics with overt features ensures that a card can be authenticated visually if equipment readers are not operating or such technologies are not functioning correctly. Overt features like color shifting technology require no special readers or equipment.

Standardization of documents (e.g., driver's license, travel documents) could be advantageous in that uniformity would simplify the inspection process as Customs and Border Control officers would know what to look for in each document. However, the government must take care not to create a system that is easy for someone to compromise. For many of the government programs being considered, standards already exist or are currently being established. Standards should define common design features while promoting a layered security system that works best for the purpose of the program. A level of commonality within the standards will aid in the training of border control officers and other government officials in looking for specific security features; however, providing some flexibility in the creation of these tools can provide an improved level of sophistication and document protection.

Electronic verification systems such as digital or RFID technology can also be positive tools in the overall document authentication and inspection process, but they are not in themselves sufficient to ensure document authentication. Recent reports about the ability of hackers to "clone" RFID technology in the new e-passports shows the vulnerability of some electronic-based technology and again validates the need to ensure a layered security system is in place rather than put our nation's security in the hands of one dominant technology.

Ease in Use of Technology

While it is necessary to layer technologies to appropriately protect against counterfeit and falsified documents; it is also important to ensure such technologies can be easily recognized and read by border control officers. Overt features such as color shift technology assist by allowing for quick and reliable visual authentication under a wide range of lighting conditions, requiring no readers or special equipment. Such ease in use would add no additional cost to the Western Hemisphere Travel Initiative or Real I.D.-compliant driver's license card verification processes.

The training of officers to correctly identify overt features like color shifting ink can be conducted by providing simple instructional materials. These can be used as a periodic training tool, or even as a guide that can be held alongside a document to verify how the technology is supposed to work.

Effect of Overt Technology on Border Traffic

To ensure border traffic is not impeded by the creation of new technology documents, it is recommended that the government find ways to validate such documents by not deviating greatly from existing operational procedures. Any additional steps to address new technology, no matter how small, will add time to the border clearance process. This concern re-emphasizes the importance of a secure overt feature that an inspector can easily validate while conducting a visual inspection of a document.

Cost Estimate for Overt Technology

When estimating the cost of various technologies it must be understood that there is a cost associated with the technology itself and the cost to appropriately utilize the technology at time of document issuance and inspection. For example, the additional cost of an e-Passport is not simply related to the cost of adding the contactless chip to a blank passport book. The true cost includes the systems to write data to the contactless chip at the time the passport is personalized plus the cost of the systems to read data from the chip at border crossings.

When considering the cost of establishing a layered security solution to documents, overt security features like color shifting ink technology is a minimal addition as there is only the cost of the formulated ink product and related printing expenses incurred during the manufacture of the document. There are no systematic costs in either the personalization or inspection of the document. As such the cost of color shifting ink is in the order of less than $0.03 per document and may be less than $0.01 per document depending on the document design and volume.

NTEU

The National Treasury Employees Union

STATEMENT OF COLLEEN M. KELLEY
NATIONAL PRESIDENT
NATIONAL TREASURY EMPLOYEES UNION

ON

IMMIGRATION AND BORDER SECURITY

SUBMITTED TO

SENATE COMMITTEE ON FINANCE
UNITED STATES SENATE
August 2, 2006

Chairman Grassley, Ranking Member Baucus, distinguished members of the Committee; I would like to thank the Committee for the opportunity to provide this testimony. As President of the National Treasury Employees Union (NTEU), I have the honor of leading a union that represents over 15,000 Customs and Border Protection Officers (CBPOs) and trade enforcement specialists who are stationed at 317 land, sea and air ports of entry (POEs) across the United States. CBPOs make up our nation's first line of defense in the wars on terrorism and drugs.

Customs and Border Protection (CBP) entry specialists, import specialist and trade compliance personnel enforce over 400 U.S. trade and tariff laws and regulations in order to ensure a fair and competitive trade environment pursuant to existing international agreements and treaties. They play a leading role in stemming the flow of illegal contraband such as child pornography, illegal arms, weapons of mass destruction and laundered money. Because CBP is also a revenue collection agency, its personnel contribute directly to the economic health of the country. In 2005 alone, CBP commercial operations personnel collected an estimated $31.4 billion in revenue on over 29 million trade entries.

When CBP was created, it was given a dual mission of not only safeguarding our nation's borders and ports from terrorist attacks, but also one of regulating and facilitating international trade; collecting import duties; and enforcing U.S. trade laws.

Currently, there are thousands of different documents that a traveler can present to CBP officers when attempting to enter the United States, creating a tremendous potential for fraud. Each day CBPOs inspect more than 1.1 million passengers and pedestrians, including many who reside in border communities who cross frequently and contribute to the economic prosperity of our country and our neighbors. At the U.S. land borders, approximately two percent of travelers crossing the border are responsible for nearly 48 percent of all cross-border trips.

On an average day, CBP intercepts more than 200 fraudulent documents, arrests over sixty people at ports of entry, and refuses entry to hundreds of non-citizens, a few dozen of whom are criminal aliens that are attempting to enter the U.S. In FY 2005, over 84,000 individuals were apprehended at the ports of entry trying to cross the border with fraudulent claims of citizenship or documents.

To determine whether someone is a U.S. citizen, CBPOs may be presented with thousands of different birth certificates (state and country) and 50 distinct drivers licenses by travelers. And in spite of the large number of daily border crossings by U.S. citizens, it is NTEU's understanding that CBPOs receive very little training at the Federal Law Enforcement Training Center on identifying fraudulent U.S. proof of citizenship documents. What training exists focuses on passports and other international documents.

The Intelligence Reform and Terrorism Prevention Act of 2004 (IRTPA), requires that by January 1, 2008, the Secretary of Homeland Security consult with the Secretary of State and develop and implement a plan to require U.S. citizens and foreign nationals to present a passport or other approved documentation to enter or re-enter the United States (Sec. 7209). This documentation must confirm both identity and citizenship before entry or re-entry can occur. Implementation of this program would reduce the numbers of identification documents that CBP Officers are required to verify, but adequate training on identification of fraudulent documents is critical now. Moreover, adequate staffing of the ports of entry is also crucial for CBP officers to meet would their duo mission of facilitating travel and trade, while at the same time securing the ports of entry from illegal entry of people or goods.

One Face at the Border Initiative

On September 2, 2003, CBP announced the misguided One Face at the Border (OFAB) initiative. This initiative was designed to eliminate the pre-9/11 separation of immigration, customs, and agriculture functions at US land, sea and air ports of entry. In practice, however, the OFAB initiative has resulted in diluting customs, immigration and agriculture inspection specialization and the resulting quality of passenger and cargo inspections has declined. Under OFAB, former INS officers that are experts in identifying counterfeit foreign visas are now at seaports reviewing bills of lading from foreign container ships, while expert seaport Customs inspectors are now reviewing passports at airports. The processes, procedures and skills are very different at land, sea and air ports, as are the training and skill sets needed for passenger processing and cargo inspection.

It is apparent that CBP sees its One Face at the Border initiative as a means to "increase management flexibility" without increasing staffing levels. The Immigration and Border Security bill passed by the House last year, requires the Secretary of Homeland Security to submit a report to Congress "describing the tangible and quantifiable benefits of the One Face at the Border Initiative...outlining the steps taken by the Department to ensure that expertise is retained with respect to customs, immigration, and agriculture inspection functions..." (HR 4437, section 105) NTEU believes that an honest report will reveal the serious negative impact on national security of this misguided program. It is NTEU's observation that without adequate training and preservation of inspection specialization skills, the OFAB initiative is destined to fail.

Staffing Shortages at the Ports of Entry

There exists a continuing shortage of staff at the 317 POEs. The President's FY 2007 budget proposal requests approximately, $4.4 billion for the Department of Homeland Security's (DHS) U.S. Customs and Border Protection Bureau. This is a 12 percent increase in CBP's budget, but the bulk of the new money is to fund the hiring of 1,500 Border Patrol agents. For salaries and expenses for Border Security, Inspection and Trade Facilitation at the 317 Ports of Entry (POEs), the budget calls for an increase of only $32 million, adding just 21 Full Time Equivalents (FTEs).

According to a recent report by the Government Accountability Office (GAO), **"as of June 2003, CBP has not increased staffing levels [at the POEs]"** and **"CBP**

does not systematically assess the number of staff required to accomplish its mission at ports and airports nationwide or assure that officers are allocated to airports with the greatest needs…(see GAO-05-663 page 19) The GAO contends further that "CBP is developing a staffing model…however the new model…will not be used to assess optimal levels of staff to ensure security while facilitating travel at individual port and port facilities, including airports." (ibid)

It is instructive here to note that the former U.S. Customs Service's last internal review of staffing for Fiscal Years 2000-2002 dated February 25, 2000, known as the Resource Allocation Model or R.A.M., shows that the Customs Service needed over 14,776 new hires just to fulfill its basic mission--and that was before September 11. Since then, the Department of Homeland Security was created and the U.S. Customs Service was merged with the Immigration and Naturalization Service and parts of the Agriculture Plant Health Inspection Service. This became the Customs and Border Protection bureau and was given an expanded mission of providing not only the first line of defense against terrorism, but also the responsibility to make sure trade laws are enforced and trade revenue collected.

CONCLUSION

Each year, with trade and travel increasing at astounding rates, CBP personnel have been asked to do more work with fewer personnel and less, training and resources. The more than 15,000 CBP employees represented by the NTEU are capable and committed to the varied missions of DHS which range from border control to the facilitation of trade into and out of the United States. They are proud of their part in keeping our country free from terrorism, our neighborhoods safe from drugs and our economy safe from illegal trade. These men and women are deserving of more resources, training and technology to perform their jobs better and more efficiently.

The American public expects its borders and ports to be properly defended. Congress must show the public that it is serious about protecting the homeland at the 317 POEs. I urge each of you to visit the land, sea and air CBP ports of entry in your states. Talk to the CBPOs, canine officers, and trade entry and import specialists there to fully comprehend the jobs they do and what their work lives are like.

I would like to thank the committee for the opportunity to submit this testimony.