AUTHENTICATED
U.S. GOVERNMENT
INFORMATION
GPO

IDENTIFICATION DOCUMENTS FRAUD AND THE IMPLICATION FOR HOMELAND SECURITY

HEARING

BEFORE THE

SELECT COMMITTEE ON HOMELAND SECURITY HOUSE OF REPRESENTATIVES

ONE HUNDRED EIGHTH CONGRESS

FIRST SESSION

OCTOBER 1, 2003

Serial No. 108–28

Printed for the use of the Select Committee on Homeland Security

Available via the World Wide Web: http://www.access.gpo.gov/congress/house

U.S. GOVERNMENT PRINTING OFFICE

96–990 PDF WASHINGTON : 2004

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) 512–2250 Mail: Stop SSOP, Washington, DC 20402–0001

SELECT COMMITTEE ON HOMELAND SECURITY

Christopher Cox, California, Chairman

Jennifer Dunn, Washington
C.W. Bill Young, Florida
Don Young, Alaska
F. James Sensenbrenner, Jr., Wisconsin
W.J. (Billy) Tauzin, Louisiana
David Dreier, California
Duncan Hunter, California
Harold Rogers, Kentucky
Sherwood Boehlert, New York
Lamar S. Smith, Texas
Curt Weldon, Pennsylvania
Christopher Shays, Connecticut
Porter J. Goss, Florida
Dave Camp, Michigan
Lincoln Diaz-Balart, Florida
Bob Goodlatte, Virginia
Ernest J. Istook, Jr., Oklahoma
Peter T. King, New York
John Linder, Georgia
John B. Shadegg, Arizona
Mark E. Souder, Indiana
Mac Thornberry, Texas
Jim Gibbons, Nevada
Kay Granger, Texas
Pete Sessions, Texas
John E. Sweeney, New York

Jim Turner, Texas, Ranking Member
Bennie G. Thompson, Mississppi
Loretta Sanchez, California
Edward J. Markey, Massachusetts
Norman D. Dicks, Washington
Barney Frank, Massachusetts
Jane Harman, California
Benjamin L. Cardin, Maryland
Louise McIntosh Slaughter, New York
Peter A. DeFazio, Oregon
Nita M. Lowey, New York
Robert E. Andrews, New Jersey
Eleanor Holmes Norton, District of Columbia
Zoe Lofgren, California
Karen McCarthy, Missouri
Sheila Jackson–Lee, Texas
Bill Pascrell, Jr., New Jersey
Donna M. Christensen, U.S. Virgin Islands
Bob Etheridge, North Carolina
Charles Gonzalez, Texas
Ken Lucas, Kentucky
James R. Langevin, Rhode Island
Kendrick B. Meek, Florida

JOHN GANNON, *Chief of Staff*
UTTAM DHILLON, *Chief Counsel and Deputy Staff Director*
DAVID H. SCHANZER, *Democrat Staff Director*
MICHAEL S. TWINCHEK, *Chief Clerk*

CONTENTS

STATEMENTS

The Honorable Christopher Cox, Chairman, Select Committee on Homeland Security
Oral Statement 1
Prepared Statement 4
The Honorable Robert E. Andrews, a Representative in Congress From the State of New Jersey 58
The Honorable Dave Camp, a Representative in Congress From the State of Michigan 49
The Honorable Peter A. DeFazio, a Representative in Congress From the State of Oregon 45
The Honorable Bob Etheridge, a Representative in Congress From the State of North Carolina 64
The Honorable Duncan Hunter, a Representative in Congress From the State of California 74
The Honorable Sheila Jackson-Lee, a Representative in Congress From the State of Texas 8
The Honorable Kendrick B. Meek, a Representative in Congress From the State of Florida 70
The Honorable Eleanor Holmes Norton, a Representative in Congress From the District of Columbia 51
The Honorable John B. Shadegg, a Representative in Congress From the State of Arizona 54
The Honorable Christopher Shays, a Representative in Congress From the State of Connecticut 60
The Honorable Louise McIntosh Slaughter, a Representative in Congress From the State of New York 74
The Honorable Lamar S. Smith, a Representative in Congress From the State of Texas 7
The Honorable Jim Turner, a Representative in Congress From the State of Texas 5

WITNESSES

The Honorable C. Stewart Verdery, Jr., Assistant Secretary, Border and Transportation Security Policy Directorate, Department of Homeland Security
Oral Statement 9
Prepared Statement 11
Mr. Joseph R. Carico, Chief Deputy Attorney General, Commonwealth of Virginia
Oral Statement 29
Prepared Statement 30
Mr. Roscoe C. Howard, Jr., United States Attorney for the District of Columbia, Department of Justice
Oral Statement 26
Prepared Statement 27
Mr. Keith M. Kiser, Chairman, American Association of Motor Vehicle Administrators
Oral Statement 35
Prepared Statement 37
Mr. Ronald D. Malfi, Director, Office of Special Investigations, General Accounting Office
Oral Statement 32
Prepared Statement 34

Mr. Paul J. McNulty, United States Attorney, Eastern District of Virginia Department of Justice
Oral Statement 21
Prepared Statement 22
Mr. John Pistole, Assistant Director for Counterrorism, Federal Bureau of Investigation
Oral Statement 16
Prepared Statement 18

MATERIAL SUBMITTED FOR THE RECORD

Questions and Responses for the Record 76

HEARING ON IDENTIFICATION DOCUMENTS FRAUD AND THE IMPLICATION FOR HOMELAND SECURITY

Wednesday, October 1, 2003

U.S. HOUSE OF REPRESENTATIVES,
SELECT COMMITTEE ON HOMELAND SECURITY,
Washington, DC.

The committee met, pursuant to call, at 1:15 p.m., in room 2318, Rayburn House Office Building, Hon. Christopher Cox [chairman of the committee] presiding.

Present: Representatives Cox, Smith, Shays, Camp, Diaz–Balart, Linder, Shadegg, Gibbons, Sessions, Hunter, Turner, Sanchez, Markey, Slaughter, DeFazio, Andrews, Norton, McCarthy, Jackson Lee, Christensen, Etheridge, Lucas of Kentucky and Meek.

Chairman COX. [Presiding.] Good afternoon, a quorum being present, the Select Committee on Homeland Security will come to order.

The committee is meeting today to consider how lax government policies toward the issuance of official identification documents, such as driver's licenses, are becoming a dangerously weak link in the war on terrorism. On September 11th, 2001, Al Qaeda slipped into airports in Boston, Newark, and Washington, D.C. undetected. No less than seven of these terrorists used authentic Virginia identification cards obtained from the Virginia Department of Motor Vehicles.

The terrorists used Virginia identification cards for a reason. Although not a single one of these terrorists was actually a lawful resident of Virginia, they knew the weaknesses of Virginia's identification process and they exploited those weaknesses in their plot to kill thousands of Americans.

Here is how they did it. In August 2001, Hani Hanjour, whose picture is on the screen, went to the DMV in Springfield, Virginia where he used a false address to obtain an identification card. And that false address of course, among other things, falsified his state of residence. Hanjour would wind up flying into the Pentagon.

The same day, Khalid Almihdhar went to the same Virginia DMV and likewise used false information to obtain his Virginia license. The next day, Hanjour and Almihdhar used their new cards to attest that a third 9/11 hijacker, Majed Moqed, lived in Virginia. That allowed him to get an identification card.

That same day they got an I.D. for a fourth hijacker, Salem Alhazmi in exactly the same way. Later in August, Hanjour signed a DMV form for Ziad Samir Jarrah. He would eventually be one

of the hijackers on United Flight 93 headed for Washington which crashed in Pennsylvania.

Abdulaziz Alomari, who crashed into the World Trade Center, also had obtained an illegal Virginia I.D. card. And so did Ahmed Alghamdi. He used his Virginia identification card to board one of the planes that hit the World Trade Center. Although none of us thought that the horrors of that day would or could ever happen, we vowed as a nation on 9/11, "Never again."

To the credit of the Commonwealth of Virginia, the governor, the attorney general and the legislature acted quickly and they changed their laws. They tightened the rules for the issuance of driver's licenses and I.D. cards to prevent further abuse and to protect their citizens. But according to a recent General Accounting Office report, even as Virginia has moved to protect the integrity of its identification system, several other states continue to administer loophole-ridden systems.

In these states, the Department of Motor Vehicles invites terrorists and criminals to create multiple fraudulent identities. And one state, California, has actually amended its laws to make things worse, introducing the very problems that Virginia had before 9/11.

In August, our friend and colleague, Representative Eleanor Holmes Norton, wrote to me and to the ranking member to request this hearing into the dangers of fraudulent I.D. cards. This is a problem she has seen first-hand in the District of Columbia and that plagues too many other jurisdictions in our nation. In particular, she stressed the problems that laxity in government identification cards creates for homeland security, and I agree.

Thank you, Eleanor, for your vigilance on this important issue.

We all know that a driver's license is the most commonly used form of identification in America. We use it to board airplanes, to buy weapons, to enter secured government facilities, to open bank accounts, to cash checks and to cross international borders. A driver's license carries a presumption of authenticity that establishes legitimacy; that is why Al Qaeda operatives here in the United States wanted them and why they still want them.

Some of the 9/11 terrorists used their true identities, others used false names. In each case, however, the pattern was the same: the terrorists found it simple to obtain genuine government-issued I.D. cards by submitting false information to a DMV. As I said, Virginia has moved swiftly to close these loopholes; California has moved to widen them.

Recently, the GAO sent three undercover agents into separate offices of the California DMV, each with false identification, purportedly from Texas, which they had manufactured themselves on a desktop computer using PhotoShop. According to the GAO, the documents should have been easily identified as forgeries. To make it especially easy for the California DMV to stop the fraud each of the three undercover agents used the same fake name. Yet California cheerfully issued California's driver's license to all three of them; all based on the same poor-quality forged documents and all using exactly the same name.

According to the GAO, California has no systems in place to detect attempts by terrorists or criminals to obtain driver's licenses, yet the DMV employees have no training in what to do with false

documents when they see them. And there is nothing to stop an Al Qaeda member or a drug runner or a common criminal from doing just what their undercover agents did to obtain a California driver's license with no legitimate backup identification.

And all of this was true before California changed its law a few weeks ago to make identity theft and fraudulent license issuance easier than ever. California's new law actually allows an individual to obtain a driver's license using documents that we know, to a certainty, are not and cannot be secure. In California, an Al Qaeda operative may now obtain a driver's license with a taxpayer identification number issued by the IRS, but the IRS has repeatedly stated that this taxpayer identification is not a reliable means to identify a person and should not be used for identification purposes.

In fact, a taxpayer identification number can be obtained by a third party; that is, you can obtain a taxpayer identification number for someone else, or someone else can obtain one in your name. And it can be obtained by mail, an applicant need not even appear in person.

For all of these reasons, the IRS has posted a warning on its website that taxpayer identification numbers do not prove identity outside the tax system and should not be offered or accepted as identification for non-tax purposes. So says the IRS, yet the state of California has now changed its law to do exactly that. It is as if 9/11 never happened.

Likewise, both the Department of Homeland Security and the FBI have stated that they have serious concerns regarding the reliability for identification purposes of the matricular consular, a sort of, "I.D. on the fly" issued by Mexican consulates in the United States. It too, is acceptable documentation to obtain a driver's license in California under the new law.

Homeland Security Secretary Tom Ridge has said that states and financial institutions that rely upon the matricular consular do so at their own risk. California has decided to incur that risk on behalf of its 30 million people so that, ironically, the state of California now accepts as secure a document that most Mexican provincial governments do not.

This is hardly a sign of post–9/11 progress in the area of securing us against the dangers of document fraud. To meet the terrorist threat, we need to get better, more reliable identification information to our customs and immigration inspectors, to state DMVs, to the TSA, and to the law enforcement security personnel and civilians who need it to ensure our safety. The Congress and this committee must consider whether it is not time for uniform minimum standards for identification to board aircraft and to purchase dangerous weapons.

Our 50 states, territories and the District of Columbia need direction from the Department of Homeland Security about the best way to defend against document fraud and identity theft. We need to continue the development of technology to help ensure more reliable identification, and we need to provide training for our local, state and Federal officers and civilian employees who check I.D.s everyday at airports, DMVs, gun shops, banks and on our borders.

In short, we need to ensure that the DHS and the Congress are doing all we can to prevent document fraud and identity theft, so

that we can keep our bi-partisan promise in the crucible of 9/11, "Never again."

PREPARED STATEMENT OF THE HONORABLE CHRISTOPHER COX, CHAIRMAN SELECT COMMITTEE ON HOMELAND SECURITY

On September 11, 2001 al Qaeda slipped into airports in Boston, Newark, and Washington, DC undetected. No less than 7 of these terrorists used authentic Virginia identification cards obtained from the Virginia Department of Motor Vehicles.

The terrorists used Virginia identification cards for a reason. Although not a single one of these terrorists was actually a lawful resident of Virginia, they knew the weaknesses of Virginia's identification process; and they exploited those weaknesses in their plot to kill thousand of Americans.

Here is how they did it. In August 2001, Hani Hanjour went to the DMV in Springfield, VA, where he used a false address to obtain an identification card. Hanjour would wind up flying into the Pentagon. The same day, Khalid Almihdhar went to the same Virginia DMV and likewise used false information to obtain his Virginia's license. The next day, Hanjour and Almihdhar used their new cards to attest that a third 9–11 hijacker, Majed Moqess, lived in Virgina. That allowed him to get an identification card. That same day, they got an ID for a 4th hijacker, Salem Alhamzi, in exactly the same way. Later in August, Hanjour signed a DMV form for Ziad Samir Jarrah. He would eventually be one of the hijackers on United Flight 93, headed for Washington, DC, which crashed in Pennsylvania. Abdulaziz Alomari, who crashed into the World Trade Center, also had obtained an illegal Virginia ID card. And so did Ahmed Alghamdi; he used his Virginia identification card to board one of the planes that hit the World Trade Center.

Almost none of us thought that the horrors of that day would or could ever happen. But in the wake of 9–11, we vowed, as a nation, "never again." To the credit of the Commonwealth of Virginia, the governor, the attorney general, and the legislature acted quickly to change their laws. They tightened the rules for the issuance of driver's licenses and ID cards to prevent further abuse, and to protect their citizens. But according to a recent General Accounting Office report, even as Virginia has moved to protect the integrity of its identification system, several other states continue to administer loophole-ridden systems. In these states, the Department of Motor Vehicles invites terrorists and criminals to create multiple fraudulent identities. And one state, California, has actually amended its laws to make things worse, and to introduce the very problems that Virginia had before 9–11.

In August, our friend and colleague, Eleanor Holmes Norton, wrote to me and the Ranking Member to request this hearing into the dangers of fraudulent ID cards. This is a problem she has seen first-hand in the District of Columbia, and that plagues too many other jurisdictions in our nation. In particular, she stressed the problems that laxity in government identification cards create for homeland security, and I agree. Thank you, Eleanor, for your vigilance on this important issue.

We all know that a driver's license is the most commonly used form of identification in America. We use it to board airplanes, to buy weapons, to enter secure government facilities, to open bank accounts, to cash checks, and to cross international borders. A driver's license carries a presumption of authenticity. It establishes legitimacy.

That is why al Qaeda operatives here in the United States wanted them—and why they still want them. Some of the 9–11 terrorists used their true identities. Other used false names. In each case, however, the pattern was the same. The terrorists found it simplicity itself to obtain genuine government-issued identification cards by submitting false information to the DMV.

While Virginia moved swiftly to close the loopholes that made this possible, California has moved to widen them. Recently, the GAO sent three undercover agents into separate offices of the California DMV—each with false identification, purportedly from Texas, which they had manufactured themselves on a desktop computer using PhotoShop. According to the GAO, the documents should have been easily identified as forgeries. To make it especially easy for the California DMV to stop the fraud, each of the three undercover agents used the same fake name. Yet California cheerfully issued California driver's licenses to all three of them—all based on the same poor quality forged documents, and all using exactly the same name.

According to the GAO, California has no systems in place to detect attempts by terrorists or criminals to obtain drivers' licenses; its DMV employees have no training in what to do with false documents when they see them; and there is nothing to stop an al Qaeda member, or a drug runner, or a common criminal from doing just what their undercover agents did to obtain a California driver's license with no legitimate backup identification.

And all of this was true before California changed its law a few weeks ago to make identity theft and fraudulent license issuance easier than ever. California's new law actually allows an individual to obtain a driver's license using documents that we know to a certainty are not, and cannot, be secure.

In California, an al Qaeda operative may now obtain a driver's license with a Taxpayer Identification Number (TIN) issued by the IRS. But the IRS has repeatedly stated that the TIN is not a reliable means to identify a person, and should not be used for identification purposes. In fact, a TIN can be obtained by a third party; that is, you can obtain a TIN for someone else, or someone can obtain a TIN in your name. And it can be obtained by mail. An applicant need not even appear in person. For all of these reasons, the IRS has posted this warning on its website:

> Since [Taxpayer Indentification Numbers] are strictly for tax processing, we do not need to apply the same standards as agencies that provide genuine identify certification. ITIN applicants are not required to apply in person; third parties can apply on their behalf; and we do not conduct background checks or further validate the authenticity of identity documents. ITINs do not prove identity outside the tax system, and should not be offered or accepted as identification for non-tax purposes.

Yet, the State of California has now changed its law, to do exactly that. It is as if 9–11 never happened. Likewise, both DHS and the FBI have stated that they have serious concerns regarding the reliability for identification purposes of the matricula consular, a sort of ID-on-the-fly issued by Mexican consulates in the United States. But it, too, is acceptable documentation to obtain a driver's license in California under the new law. Homeland Security Secretary Ridge has said that states and financial institutions that rely upon the matricula consular do so "at their own risk." California has decided to incur that risk on behalf of its 30 million people; so that, ironically, the State of California now accepts as secure a document that most Mexican provincial governments do not.

This is hardly a sign of post 9–11 progress in the area of securing us against the dangers of document fraud. To meet the terrorist threat, we need to get better, more reliable identification information to our Customs and Immigration inspectors, to state DMVs, to the TSA, and to the law enforcement, security personnel, and civilians who need it to ensure our safety. The Congress, and this Committee, must consider whether it is not time for uniform minimum standards for identification to board aircraft, and to purchase dangerous weapons.

Our 50 states, territories, and the District of Columbia need direction from the Department of Homeland Security about the best way to defend against document fraud and identity theft. We need to continue the development of technology to help ensure more reliable identification. And we need to provide training for our local, state and federal officers and civilian employees who check identifications every day at airports, DMVs, gun shops, banks, and on our borders.

In short, we need to ensure that the DHS and the Congress are doing all we can to prevent document fraud and identity theft, so that we can keep our bipartisan promise in the crucible of 9–11, "Never Again."

The chair now recognizes Mr. Turner, the ranking Democrat member, for any statement that he may have.

Mr. TURNER. Thank you, Mr. Chairman.

As you stated, we all saw the results of Al Qaeda's ability to obtain driver's licenses in at least five different states through fraudulent means and the consequences that flowed from that. We were all surprised, as you stated, Mr. Chairman, when the General Accounting Office did its investigation and was able to have several undercover agents enter the United States with counterfeit documents with few questions asked.

So it is clear to us, I think, that today we must move faster and we must be much stronger, in terms of our effort, to end the use of fraudulent documents, particularly those that are used to cross our borders and enter our country. We know that the forgers can produce high-quality birth certificates and driver's licenses with off-the-shelf software. It is certainly very difficult for our border agents to be able to deal with the problem when there are over 240 different types of valid driver's licenses issued in the United States

today and more than 50,000 different versions of birth certificates issued by states and counties and cities.

It is unlikely that these officers and inspectors can become with familiar with these valid forms of identification without spending years and years on the job. Past attempts to reduce fraudulent documents have met with mixed results. Some years ago, the Congress made an effort to develop a more secure social security card but, after several different types of cards were proposed, no action was taken.

Clearly, the Congress and the American people have had an aversion to any form of uniform identification. It does seem incumbent upon us, however, to revisit the issue, to look more carefully at providing uniform standards for at least state driver licenses so that we can begin to make some inroads upon a very serious problem that places our nation at risk.

We hope we can learn from the testimony today whether there are sufficient programs in place for our Federal border officers and state and local law enforcement to detect document fraud, whether planned programs such as the U.S. VISIT Entry–Exit System will truly help to deter and eliminate the use of fraudulent documents at our borders, and whether legislative remedies, perhaps expanding criminal penalties for document use, will be appropriate in fighting this very difficult problem.

We also need to consider whether the Federal Government should provide more direction and/or assistance to the states in developing more secure official identification documents. Hopefully, these issues and others will be addressed by our distinguished panel today.

I would also like to join the Chairman in thanking Eleanor Holmes Norton for her suggestion that this Committee conduct a hearing on this very critical issue. I appreciate Eleanor's leadership in this area and her work on the issue.

Thank you, Mr. Chairman.

Chairman COX. I thank the gentleman.

Under Committee Rule Three, members who waive an opening statement can add 3 minutes to their time for questioning. Does any member wish to make an opening statement?

Ms. Norton?

Ms. NORTON. Mr. Chairman, may I thank you and our ranking member for today's hearing in response to illegal document buying and selling in the nation's capital, this region, and in the country post–9/11.

The District of Columbia may be the last place to expect open and notorious hawking of counterfeit birth certificates, driver's licenses and social security cards. Such activities have long been associated with the Southwest and border communities because of the presence of large numbers of undocumented immigrants.

In the District, the sale of illegal documents has been concentrated in Adams Morgan, a neighborhood with many immigrants from El Salvador, Guatemala and all Latin and Central American countries. D.C. Councilmember Jim Graham, who first brought this matter to my attention, and neighborhood residents complained of constant street corner harassment and compared the effect on residents to harassment by drug peddlers. However, it

doesn't take much imagination after September the 11th to see how illegal activities directed toward immigrants seeking identification papers necessary to find work in this country could become a conduit for people seeking identification documents to enable them to carry out terrorist activities.

We know that several of the 9/11 terrorists had driver's licenses, they were from Saudi Arabia, not Latin America. The lesson of 9/11 is to read the handwriting on the wall, not to wait until, to quote, the moving finger, having writ, writes and moves on. We need a hearing from officials from the national capital region where the vulnerability that carries elements is perhaps, the most calming effect.

Our particular report shows the efforts of our U.S. Attorney Roscoe Howard, whose office has been chosen to prosecute cases. The ways the document-producing mills have lined up the street corner puddles have apparently limited three of the four recent document readings. Nevertheless, I will not be surprised to find illegal document sales still occurring this afternoon in Adams Morgan. The councilman tells me that that process is continuing.

I don't blame the states. Get them pressures and empowerments occur in the States, and we can expect that they would have different approaches. Particularly, this issue cries out for National Homeland Security leadership.

One of the problems may be that we are over-independent on two 9/11 memos; blanketing the area with agents, rough and the like. Much of that cries for priority, so our particular problems in the nation's capital. I recognize that there may never be enough agents to eliminate the problem on a retail basis. This problem is national in scope, and therefore, needs new national approaches. Perhaps, for example, increasing penalties and the use of jail term, plus deportation; penalties have been used in prosecutions here, instead of deportation only.

Today the issue is not pre–9/11 document selling to immigrants, but post–9/11 violations that carry great homeland security risks. We, therefore, need new thinking and remedies. And I hope we can use today's hearing to encourage new approaches of new thinking outside the box to get a tightening around the issues before it emerges in a new and lethal form.

May I thank you again, Mr. Chairman, and our own ranking member as well.

Chairman COX. Thank you.

The gentleman from Texas?

Mr. SMITH. Mr. Chairman, I will be brief, but I also want to just mention a couple things because I am going to have to leave at 2 o'clock for a conference and I may not be able for questions.

First of all, I want to thank you for convening this hearing, and I particularly want to thank you for a very tough statement. I hope our friends in the administration in fact, listen to your statement, and perhaps will act on it. We had the unfortunate situation recently where the Department of Treasury has encouraged individuals and banks and organizations to rely upon one of those documents that you identified as unreliable, the matricular cards. And they do so, in my judgment, at great danger to the American peo-

ple. So I hope the administration will reconsider what they have chosen to do with those matricular cards.

That decision was made, by the way, against the advice of the Department of Justice and the Homeland Security Committee and many of us in Congress. So I hope the administration, as I say, will reconsider. But I appreciate the hearing today and yield back.

Chairman COX. Does any other member wish to be recognized?

PREPARED STATEMENT OF THE HONORABLE SHEILA JACKSON-LEE

we are living in a high-tech world. It is tempting to believe that the problem of fraudulent documents can be solved with technology, but two recent government reports indicate that the human factor must be addressed first. On January 30, 2003, the General Accounting Office (GAO) reported the results of an investigation it had performed at the request of the Senate Committee on Finance. The Finance Committee was concerned about the illegal transportation of currency through our borders, especially counterfeit money and terrorism funds. It asked the agents of the Office of Special Investigations at GAO to attempt to enter the United States as United States citizens from Canada, Mexico, and Jamaica at land, air, and sea ports of entry using fictitious identities and counterfeit identification documents.

the GAO agents encountered no difficulty entering the United States. From September 2002, through May 2003, they used counterfeit documentation, including counterfeit driver's licenses and fictitious names, to enter the United States from Jamaica, Barbados, Mexico, and Canada. Bureau of Immigration and Customs Enforcement (BICE) staff never questioned the authenticity of the counterfeit documents.

In other tests, GAO agents obtained Social Security numbers for fictitious children when investigators posed as parents of newborns and submitted counterfeit birth certificates and baptismal certificates. GAO agents breached the security of airports and Federal office buildings because no one questioned the authenticity of their counterfeit identification. In still another test, GAO agents used counterfeit driver's licenses with fictitious identifiers to purchase firearms from Federal firearm licensees in five states. The weapons purchased included (1) a 9mm stainless semiautomatic pistol, (2) a .380 semiautomatic pistol, (3) a 7.62mm Russian-manufactured rifle, (4) a .22 caliber semiautomatic rifle, (5) a 9mm semiautomatic pistol, and (6) a .25 caliber semiautomatic pistol.

In February of 2003, the Inspector General (IG) of the Justice Department issued a similar report which sheds additional light on the reason for the difficulties identified by the GAO study. The only part of the IG's report that can be discussed in public is the Executive Summary. According to the Executive Summary, the capability of immigration inspectors to analyze advance passenger information to identify high-risk and inadmissible travelers is limited by a lack of adequate resources. The lookout system for spotting high-risk and inadmissible travelers does not always provide primary inspectors with available, critical information. Primary inspectors were not always querying lookout databases as required, and controls were not sufficient to ensure that all primary inspectors and supervisors could access backup information in the event of system outages.

The report also mentions the fact that INS invested more than $19 million in Fiscal Year 2002 to provide basic training for approximately 1,000 new immigration inspectors. The IG found that the training provided a good foundation for newly hired inspectors, but it was insufficient in two important areas, on the use of computer systems that provide lookouts and other critical information and on awareness of current terrorist tactics used to enter the United States.

I know from personal experience that there is a serious problem with the recruitment and retention of immigration inspectors. It is common for the immigration inspection stations at Houston's international airport to be understaffed. Making matters worse, many of the inspectors are inexperienced. In Fiscal Year 2002, approximately 26 percent of all inspectors at air, land, and sea ports of entry were newly hired.

I hope that today's hearing will lead to the development of new, more effective ways to train and equip the security personnel in our country who are charged with the responsibility of detecting fraudulent documents. Thank you.

Chairman COX. If not, we have a very distinguished panel of witnesses today. I would ask each of our witnesses to summarize your

testimony as you see fit because you were good enough to provide us with your written statements in advance of this hearing and members have your written statements, and they will be included in the record.

I will introduce our first witness. He is the assistant secretary of the Department of Homeland Security for Border and Transportation Security Policy, Hon. C. Stewart Verdery, Jr.

Mr. Verdery?

STATEMENT OF THE HONORABLE C. STEWART VERDERY, JR., ASSISTANT SECRETARY, BORDER AND TRANSPORTATION SECURITY POLICY DIRECTORATE, DEPARTMENT OF HOMELAND SECURITY

Mr. VERDERY. Chairman Cox, ranking committee member and other distinguished members of the committee, I am pleased to be here today to testify about homeland security and the potential threat of terrorism imposed by document fraud, identity theft, and the misuse of social security numbers.

The Department of Homeland Security and the Border and Transportation Security Directorate, Directorate in particular, are actively working to address these critical issues. As you mentioned, I am the assistant secretary for policy and planning within BTS. BTS is responsible for maintaining the security of our nation's borders and transportation systems.

My office supervises and coordinates policy development for all the BTS agencies which includes the Transportation Security Administration, the Bureaus of Customs and Border Protection and Immigration and Customs Enforcement, the Federal Law Enforcement Training Center and the Office of Domestic Preparedness, and we work closely with the Secret Service and the Coast Guard within DHS.

Let me detail briefly some of the steps that DHS and BTS are taking to address document fraud and identity theft. First and foremost, DHS deploys first-rate people at our ports of entry. They do a terrific job at detecting the use of fraudulent documents and conducting the resulting investigations.

Through early September of this fiscal year which ended yesterday, our officers at the Bureau of Customs and Border Protection, CBP, had intercepted over 60,000 fraudulent documents at over 300 ports of entry.

As Secretary Ridge has announced, DHS is unifying the border inspection process by establishing the CBP officer, an officer who will be cross-trained to handle immigration, customs and agricultural inspection needs. All CBP inspectors will receive our most current training in identifying fraudulent and altered documents.

DHS and BTS are leveraging its expertise overseas as well. Officials at the Bureau of Immigration and Custom Enforcement, or ICE, their Forensic Document Lab, have trained over 6,400 law enforcement officials around the world on how to detect fraudulent documents this fiscal year, and we have published over 120 Document Alerts, a 50-percent increase from last year.

These short, easy-to-understand document alerts are sent to the field overseas so that inspectors and law enforcement authorities can concentrate on one or two known features of an identity docu-

ment that criminals are trying to exploit. And I brought one example to my right of one such alert concerning the misuse of the Iraqi "N" Series passports, and these passports were available for purchase in Turkey for about $500.

Second, the Department employs first-class investigators at ICE and at the Secret Service who investigate cases of document fraud and identity theft. As you will hear today from the United States Attorneys for the District of Columbia and for the Eastern District of Virginia, ICE and Secret Service agents have played and will play a key role in the interagency process and task forces that have been formed to investigate and prosecute these types of cases.

ICE investigators have logged hundreds of thousands of hours working on counterfeit document related investigations. The primary focus in these cases is to detect, deter, disrupt and dismantle major criminal enterprises operating not only in the United States, but around the world as well. These cases often entail long-term, complex investigations that involve our international partners.

I would like to share briefly the preliminary results of one of ICE's ongoing investigations, the Operation Card Shark investigation mentioned in the testimony, and I will leave the details to U.S. Attorney Howard, who will be after me in a couple of minutes.

With the investigation continuing today, four document mills have already been closed, close to 2,000 documents have been seized, 50 aliens have been arrested, 30 have been removed from the United States and 15 have been prosecuted.

The Secret Service is also demonstrating success in this area. This fiscal year, the Secret Service has made 209 arrests in cases involving identity theft. These cases reflect actual losses to consumers of about $5 million and a potential loss of $23 million.

This summer the Secret Service developed and distributed to state and local law enforcement agencies throughout the United States an Identity Crime Video in CD–ROM. This CD–ROM contains over 50 investigative and victim assistance resources that state and local law enforcement officers can use with combating identity crime. They have authorized that as many copies to be made of this as possible to get the word out as broadly as we can.

And just to give credit where credit is due, this CD–ROM was made in collaboration with the Postal Inspection Service, the Federal Trade Commission and our partners at the International Association of Chiefs of Police.

Third, in responding to Congressman Turner's point, the U.S. VISIT Program, we will be changing—

Chairman COX. If I could ask you to summarize.

Mr. VERDERY. Sure, of course.

Chairman COX. Because your 5 minutes has expired.

Mr. VERDERY. Sure.

We are changing the way we do business at our ports of entry. This critical tool will capture point of entry and exit information by visitors to the United States using biometrics. We will be locking in people's identity when they arrive for the first time and when they exit. We will also know when they return.

And with that, I will lastly like to mention we are working closely with representatives from the Social Security Administration to

discuss issues of mutual concern; how to reduce instances of misuse of social security numbers.

On behalf of Secretary Ridge and Undersecretary Hutchinson, I look forward to questions you might have.

Thank you.

[The statement of Mr. Verdery follows:]

PREPARED STATEMENT OF THE HON. STEWART VERDERY, JR.,

Chairman Cox, Ranking Member Turner, and other distinguished members, I am pleased to be here today to testify about homeland security and the potential threat of terrorism presented by document fraud, identity theft, and the misuse of Social Security Numbers.

As you know from Congressional hearings, GAO investigations, and press reports, it is certainly possible today to produce or acquire false documents and gain entry into the United States. The Department of Homeland Security and the Directorate of Border and Transportation Security are working actively to address this problem in a number of ways, as I will detail in my testimony.

Despite all these good efforts, we, and the Congress, must be realistic about the results to expect. While we can, over time, reduce the instances when false or fraudulent documents are used to enter the U.S. or to obtain some governmental benefit, there is no easy fix available, and this is a long-term issue for the Congress, the Administration, and DHS to work through together.

DHS is working diligently on all these issues. My staff has had several meetings with the Social Security Administration (SSA) to discuss issues of mutual concern and potential ways to reduce the instances where Social Security Numbers are misused.

We are also working with State and Local government authorities, and non-government entities like the American Association of Motor Vehicle Administrators (AAMVA) on issues of mutual concern.

Description of the Problem

Document Fraud

Fraudulent documents, and, equally as important for the purposes of this hearing and our enforcement efforts, legitimate documents issued as a result of the use of fraudulent "breeder" documents can and are likely used to gain entry into the U.S. and to obtain federal and state governmental benefits each and every day.

As a general rule, the Immigration and Nationality Act requires all U.S. citizens to present a valid U.S. passport to enter or leave the U.S. There are several exceptions to this general rule. The most important applies to travel to and from the U.S. involving "any country, territory, or island adjacent [to the U.S.] in North, South, or Central America excluding Cuba." Thus, as a matter of law, U.S. citizens do not typically need to present a single document—a passport—to reenter the U.S. for any travel in the Western Hemisphere.

As a U.S. citizen is not required to present a passport for reentry, federal regulations do not detail what is necessary to validate a person's claim to citizenship in a manner equivalent to that of a passport.

The law requires that a person claiming to be a U.S. citizen "must establish that fact to the examining officer's satisfaction." [8 C.F.R. 235.1(b).]

In operational practice, our inspectors, now called "officers," from the Bureau of Customs and Border Protection (CBP) examine any document that may establish identity and place of birth, such as a U.S. birth certificate, driver's license, or whatever else the person's basis for claiming citizenship might be, including baptismal certificates, Certificate of Naturalization, Report of Birth Abroad of U.S. Citizen, or Certificate of Citizenship.

No law or regulation prevents an oral claim of U.S. citizenship in these circumstances. An inspector may, and often does, ask for documentation to support a claim, but this is not currently required. Thus, even if an individual lacks any documentary identification or the person presents counterfeit documents, inspectors must let the individual back into the U.S. if the inspector is satisfied that the individual really is a U.S. citizen.

Although the government may be able to prosecute the individual for using a counterfeit document, the use of the counterfeit document by a U.S. citizen, in and of itself, is not a sufficient ground for preventing the U.S. citizen from lawfully reentering.

Let me be clear about one thing. CBP officers do not accept or rely on a State-issued driver's license as sufficient proof of legal presence in the U.S even though a person will often present his or her license as an identity document. But, it is also

true, that officers consider a validly issued driver's license as one piece of information in the total information the officer considers in making a judgment about a person's right to have a legal basis to reenter the U.S.

The 21 States that currently issue driver's licenses without requiring proof of legal status in the U.S. thus complicate the work of our officers who examine some ½ billion identity documents each and every year. The officers who review these licenses must ask for additional information or pose additional questions to the person presenting the license since the fact of holding the driver's license does not confer on the license holder a legal basis for being present in the U.S.

By law and practice, CBP officers cannot focus their detection efforts on a single document, such as the passport, and concentrate their expertise on recognizing and blocking the fraudulent use of this one document or type of document. As other witnesses have testified before Congress, there are more than 240 different types of valid driver's licenses issued within the United States, and more than 50,000 different versions of birth certificates issued by U.S. States, counties, and municipalities.

Even excluding baptismal records, it would not be easy for CBP officers to have a passing familiarity with, let alone a working knowledge of, each of these documents. While advances in technology allow our dedicated and hardworking CBP officers to examine and validate documents presented for reentry, that same technology also enables the perpetrators of fraud to produce, relatively inexpensively, high-quality fraudulent documents. Forgers and counterfeiters can produce high-quality fake birth certificates and driver's licenses with off-the-shelf software programs and materials that are difficult to detect without sensitive instruments and sufficient time to examine them.

Our inspectors are also charged with detecting look-a-likes or impostors who attempt to use valid documents which belong to another person. This is one of the fastest growing phenomena in travel document abuse. Document vendors solicit genuine, unaltered documents and match them up with "look-a-likes." The Bureau of Immigration and Customs Enforcement (ICE) and CBP have developed a training program to detect impostors, which it has conducted for both U.S. and foreign immigration and border officers around the world.

Equipment costs money, and taking the time to examine thoroughly and in-depth every one of the approximately 460 million identity documents presented at our over 300 land, sea, and air ports of entry would be an enormous undertaking with potentially serious secondary effects. And, even were we to do this, this effort would only permit us to detect fraudulent documents, not, as I will discuss now, legitimately issued documents that are based on identity theft.

Identity Theft

Identity crime is the theft or misuse of an individual's personal or financial identifiers in order to facilitate other criminal activity or to gain something of value. Types of identity crime include identity theft, credit card fraud, bank fraud, check fraud, false identification fraud, and passport/visa fraud. Identity crimes are frequently associated with other crimes such as narcotics and weapons trafficking, organized crime, mail theft and fraud, money laundering, immigration fraud, and terrorism.

The topic of identity theft is intimately connected with document fraud. As the GAO and others have shown, it is quite easy today either to obtain or produce using sophisticated software and equipment fraudulent identification documents, such as a driver's license or birth certificate, or to obtain valid documents issued by the appropriate authority (again, driver's licenses, social security cards, etc.) on the basis of false or fraudulent information. For example, it would be relatively easy for an individual to obtain a properly-issued State driver's license in the name of Asa Hutchinson if the individual could establish on the basis of false documents that their name was Asa Hutchinson.

Advances in technology and the explosion of e-commerce have produced enormous advantages for people around the world, and have also conferred benefits on criminals. Information collection has become a common byproduct of e-commerce transactions. Internet purchases, credit card sales, and other forms of electronic transactions are being captured, stored, and analyzed by businesses seeking to find the best customers for their products. This wealth of available personal information creates a target-rich environment for today's sophisticated criminals, many of whom are organized and operate across international borders and include both domestic and international organized criminal groups, street gangs, convicted felons, and terrorists.

The personal identifiers most often sought by criminals are those generally required to obtain goods and services on credit. These are primarily social security numbers, names, and dates of birth. Identity crimes also involve the theft or misuse

of an individual's financial identifiers such as credit card numbers, bank account numbers and personal identification numbers.

Many identity thieves use information obtained from company databases and web sites. One case investigated by the United States Secret Service, the primary DHS agency with jurisdiction over ID theft matters, involved an identity criminal accessing public documents to obtain the social security numbers of military officers. In some cases, the information obtained is in the public domain while in others it is proprietary and is obtained by means of a computer intrusion.

The method that may be most difficult to prevent is theft by a collusive employee. Individuals or groups who wish to obtain personal or financial identifiers for a large-scale fraud ring will often pay or extort an employee who has access to this information through their employment at workplaces such as a financial institution, medical office, or government agency.

Another case, investigated primarily by ICE and the Secret Service demonstrates the nexus between identity theft and document fraud. In this Greenville, South Carolina case, male foreign nationals from Pakistan, India, and Tunisia already in the U.S. traveled to South Carolina to participate in arranged marriages, for the purpose of acquiring legal permanent residence. The "brides" and "grooms" fraudulently obtained South Carolina State and/or immigration identification documents utilizing breeder documents in order to substantiate their marriage. The "brides" were paid between $1,000 and $6,000 to enter into the "marriage." Nearly all the brides arrested signed, sworn statements admitting to their involvement in sham marriages. This case is ongoing and has resulted in over 100 arrests.

The Secret Service, ICE, the U.S. Marshal's Service, the U.S. Postal Inspection Service, the Social Security Administration's Office of Inspector General, and the South Carolina Law Enforcement Division (SLED) have all participated in this investigation.

Identity crime affects all types of Americans, regardless of age, gender, national origin, or race. Victims include restaurant workers, telephone repair technicians and police officers, to corporate and government executives, celebrities and high-ranking military officers.

Of course, and of most relevance to this hearing, fraudulent "breeder" documents obtained through identity theft can then be used to obtain genuine documents from Departments of Motor Vehicles, the Social Security Administration, and elsewhere. These legitimately issued documents can—and are—subsequently used to obtain government services and benefits and to gain reentry into the United States. There is no technology available to CBP officers—and none that I am aware of that exists anywhere—that would enable an inspector to determine that a legitimately issued document was actually based on a false breeder document presented to another government agency.

How DHS is Addressing the Problem

DHS is actively addressing these issues to make it harder for individuals—especially terrorists—to slip into the U.S. using fraudulent documents and to pursue identity thieves and those who use false breeder documents. We also vigorously investigate cases involving the use of fraudulent documents and cooperate with other federal, state, and local governmental entities, as well as the private sector, to heighten awareness and to reduce our vulnerabilities.

DHS uses a combination of advance information about individuals entering the U.S., pre-screening, registration systems such as the National Security Entry-Exit Registration System (NSEERS), and will use advanced technology, including the use of biometric information that will be incorporated into our US VISIT entry-exit system.

One Face at the Border

Training CBP officers to recognize fraudulent documents is another important step, and one that BTS takes very seriously.

Last month, Secretary Ridge announced that DHS will unify the border inspection process under one Customs and Border Protection Officer, an officer cross-trained to address immigration, customs, and agricultural inspection needs. We will have one face in one uniform—a single officer trained for primary inspection as well as how to determine who needs to go through secondary inspections.

And since we know that Al Qaeda is interested in entering our ports illegally, this officer—now trained in all three areas of inspection and armed with the best intelligence we have—improves our ability to spot and stop terrorists quickly and keep them out. We have already recruited our first group of CBP officers, who will be trained throughout this fall. For DHS, this is another significant step toward our efforts to retool where it makes sense and create efficiencies and unity around a single mission.

All CBP officers will receive our most current training on identifying fraudulent and altered documents. CBP secondary officers will receive more advanced training, and BTS will continue to maintain the world-class excellence of the ICE Forensic Document Lab (FDL), that was previously housed at the INS.

Our CBP officers are doing a good job on this issue, and will continue to improve. As of early September, CBP officers had intercepted over 60,000 fraudulent documents at our over 300 ports of entry in Fiscal Year 2003.

ICE Resources

The sole mission of the FDL, a fully-accredited crime laboratory, is to detect and deter domestic and international travel and identity document fraud, and the FDL has developed an unparalleled expertise in the area of domestic and international travel and identity fraud.

The ICE FDL maintains a collection of exemplar documents, including birth certificates, passports, and driver's licenses to differentiate valid documents from fraudulent ones. The FDL provides real-time assistance to field personnel in identifying fraudulent documents, produces and broadly distributes Document Intelligence Alerts (high quality photographic bulletins), develops and presents training programs in the detection of fraudulent documents, and works with other Federal, state, local agencies, and foreign governments to promote common efforts to combat international document fraud.

I want to mention two such samples of these ICE FDL alerts which I commend to the Members of this Committee. These alerts present, in a clear and simple format, particular features to look for in order to determine whether particular types of documents are fraudulent or counterfeit.

One alert discusses stolen blank Philippine Passports and the other concerns counterfeit Iraqi "N" series passports that were available for purchase in Turkey for about $500. The alerts highlight how to distinguish immediately between the genuine and counterfeit document.

The FDL has on file intelligence reports of over 100,000 stolen blank, genuine, passports. These passports pose a serious potential threat to national security since they are genuine documents. The FDL has developed a reference guide that contains very precise information on the issuance process of passports and country specific intelligence information. The guide is extremely useful in identifying individuals in possession of these stolen passports.

DHS is leveraging this expertise overseas, as well. In 2003, FDL officials trained over 6,400 enforcement officials around the world how to detect fraudulent documents this fiscal year, and published over 120 Document Alerts, a 50 percent increase over last year.

ICE also operates a Law Enforcement Support Center in Vermont to assist state and local law enforcement officers who have questions about identification assessments during traffic stops. In addition, ICE operates units to link enforcement and intelligence resources with adjudication officers from the Bureau of Citizenship and Immigration Services (CIS) who must make determinations about documents that they are presented for adjudication.

In addition to the work of the FDL, ICE law enforcement agents investigate cases of documents and benefits fraud. ICE has joined the U.S. Attorney's Office in the Eastern District of Virginia in a pilot project to investigate and prosecute large immigration, visa, and identification document frauds. The task force includes the participation of the Secret Service, CIS, FBI, Social Security Administration's Office of Inspector General, IRS-Criminal Investigation, Department of State, Department of Labor, U.S. Postal Inspection Service, Virginia DMV, and the Fairfax County Police Department.

ICE investigators have logged hundreds of thousands of hours working on counterfeit document related investigations. The primary focus of these cases is to deter, disrupt, and dismantle major criminal enterprises operating not only in the United States, but in source and transit countries as well. The cases often entail long-term, complex investigations that frequently involve our international partners.

Operation Card SharkI would also like to share the preliminary results of ICE's ongoing investigation, here in Washington, D.C., known as Operation Card Shark. Card Shark focuses on the street sale of counterfeit documents in the Adams Morgan area. Although the investigation continues, four document mills have already been closed resulting in the seizure of close to 2,000 documents with an estimated total street value of $155,000. 50 aliens have been taken into custody—30 have been removed from the U.S. and 15 have been prosecuted.

On July 15th, one of the primary targets of this operation was sentenced in U.S. District Court to a total of 52 months in prison for his role as a kingpin in the counterfeit document-manufacturing ring.

Card Shark has disrupted the activity of three significant organizations that operate on the North side of Columbia Road and the return of Pigeon Park to the residents of Adams Morgan.

I look forward to sharing more such successes with you in the months ahead.

US-VISIT

US-VISIT is a crucial new border security and enforcement tool that will capture point of Entry and Exit information by visitors to the United States. This system will be capable of using information, that may be coupled with biometric identifiers, such as photographs and fingerprints—to create an electronic check-in/check-out system for people who come to the United States to work or to study or visit. US-VISIT will also provide a useful tool to law enforcement to find those visitors who overstay or otherwise violate the terms of their visas and will allow us to lock-in an individual's identity, what those in the field call "positive identification" when the individual registers with US-VISIT.

By January 1, 2004, when a foreign visitor flies into one of our international airports or arrives at a U.S. seaport, the visitor's travel documents will be scanned.

Through US-VISIT, all border officers at air and some sea ports of entry will have the capability to access and review the visa information, including the photograph, during a visa holder's entry into the United States. This will enable the border officers to verify the visa photograph with the passport photograph and the individual of the visa holder during their inspection for entry into the United States. Additionally, border officers will capture biometric data to verify and lock-in select visa holders identities. The US-VISIT system will be able to compare the captured fingerprint against a fingerprint watch list. This will be an enhancement to the existing name check or biographical lookout check.

This information will become part of a foreign visitor's ongoing travel record, so their correct information can follow them wherever they go. The information will be made available to inspectors, agents, consular officials and others with a true need to know.

Mr. Chairman, we should all be clear on my next point. Good information does not threaten immigration. Quite the contrary. The more certain we are about someone's status, the less likely we are to make a mistake that would jeopardize their status—or our safety.

NSEERS

The NSEERS program requires certain nonimmigrant aliens from designated countries to be fingerprinted, interviewed, and photographed by CBP at our ports of entry at the time they are applying for admission to the United States. In addition, other aliens who are identified from intelligence sources or who match certain pre-existing criteria may also be enrolled in NSEERS.

NSEERS helps to secure our borders, by intercepting terrorists and criminals at our ports of entry, identifying aliens who deviate from their stated purposes once they enter the U.S., and identifying aliens who have overstayed their visas and are in the country illegally. DHS officers have made every effort to minimize the inconvenience for those individuals required to register, with an average processing time of just 18 minutes.

During the enrollment process, specific biographic information, itineraries and addresses are collected. If aliens remain in the U.S. for longer than 30 days, they must return to a DHS office to confirm their address and activities in the United States. Registrants must also complete a departure check when they leave the country and register with NSEERS if they are subject to registration and have not already registered.

The NSEERS registration process enables DHS to verify that an alien is living where he said he would live, and doing what he said he would do while in the United States, and to ensure that he is not violating our immigration laws.

Identity Theft

DHS is also working hard to reduce the incidence of identity theft, and the Secret Service is leading this effort on behalf of the Department.

This summer, the Secret Service developed and distributed to state and local law enforcement agencies throughout the United States an Identity Crime Video/CD–ROM. The CD–ROM I am holding contains over 50 investigative and victim assistance resources that local and state law enforcement officers can use when combating identity crime. This CD–ROM contains a short video that can be shown to police officers at their roll call meetings and discusses why identity crime is important, what other departments are doing to combat identity crime, and what tools and resources are available to officers. The Identity Crime CD–ROM is an interactive resource guide that was made in collaboration with the U.S. Postal Inspection Service, the Federal Trade Commission and the International Association of Chiefs of Police.

The Secret Service has authorized law enforcement agencies to make as many copies of the CD–ROM as they wish so that the agencies can distribute this resource to their officers to use in identity crime investigations.

The Secret Service is also training state and local law enforcement agencies to prevent identity theft the old fashioned way. In a joint effort with the Department of Justice, the U.S. Postal Inspection Service, the Federal Trade Commission and the International Association of Chiefs of Police, the Secret Service has hosted Identity Crime training seminars for law enforcement officers in New York, Chicago, Seattle, Dallas, Las Vegas, Washington D.C., Phoenix, Richmond, and Iowa, Mr. Chairman. The Secret Service has additional seminars planned for San Antonio, Texas next month, Orlando, Florida in November, and San Diego, California. These training seminars focus on providing local and state law enforcement officers with tools and resources that they can immediately put to use in their investigations of identity crime. Additionally, officers are provided resources that they can pass on to members of their community who are victims of identity crime.

Collaboration

DHS is also collaborating with others in both the government and in the private sector to combat and address these important issues. We have worked closely with the Department of State on visa issuance issues and obtaining access to the Consolidated Consular Database. My staff has met several times with representatives of the Social Security Administration (SSA) to discuss issues of mutual concern and to explore how to reduce the instances of the misuse of social security numbers.

ICE and CIS has also worked cooperatively with the SSA for a number of years through the Systematic Alien Verification for Entitlements (SAVE) Program. The SAVE program enables Federal, state, and local government agencies to obtain immigration status information to determine an applicant or recipient's eligibility for many public benefits. The SAVE Program also administers employment verification pilot programs that enable employers quickly and easily to verify the work authorization of newly hired employees.

Current SAVE participants include the SSA; National Aeronautics and Space Administration (NASA); the Department of Defense Manpower Data Center; Arizona County Health Care Cost Containment; the California and Wyoming Departments of Motor Vehicles; the New Jersey Department of Law and Public Safety, Division of Gaming Enforcement; the Mohegan Tribal Gaming Commission; and the Texas Department of Health, Asbestos Licensing Program.

The Secret Service has worked closely with the American Association of Motor Vehicle Administrators (AAMVA) to support AAMVA's efforts to develop minimum and uniform standards for U.S. driver's licenses. I understand, for example, Mr. Chairman, that there are still four states that do not require a photograph on their state's driver's license, which, obviously, makes that document easier to use in a fraudulent manner.

Secret Service representatives work closely with the private sector on a number of efforts, and, together with the private sector, formed the Document Security Alliance as an ad hoc working group of law enforcement and industry focused on developing standards for the improving the security and traceability of plastic identification cards.

Conclusion

In sum, Mr. Chairman, DHS recognizes the enormity of the problems that we face, and we are working actively to improve our ability to detect fraudulent identification documents and to keep criminals and potential terrorists from obtaining these documents in the first place.

Chairman COX. Thank you, Mr. Verdery.

Our next witness is Mr. John Pistole, who is the Assistant Director of the Federal Bureau of Investigation for Counterterrorism. We appreciate you being with us today and look forward to your testimony.

STATEMENT OF MR. JOHN PISTOLE, ASSISTANT DIRECTOR FOR COUNTERTERRORISM FEDERAL BUREAU OF INVESTIGATION

Mr. PISTOLE. Thank you, Chairman Cox.

Good afternoon, Ranking Member Turner, and other members of the committee. I appreciate the opportunity to be here today and represent the FBI in this hearing today.

As the committee is well aware, the top priority for the FBI is the prevention of the next terrorist act here in the U.S. or against U.S. interests overseas in connection with our overseas partners. More than 29,000 employees of the FBI are working toward that goal on a daily basis. The identification of sleeper cells here in the U.S. is one of the key aspects to the success in this ongoing war against terrorism. And for that, we need strong authentication procedures for issuing identifications across the country.

As we know, identity fraud is not a new problem. For those who are familiar with either the book or the movie, "Catch Me if You Can," starring Tom Hanks, as the FBI agent, of course, the good guy, we went back 40 years. We have a history of individuals who have either as a fugitive or as a fraudster used false identities to further their own goals.

The significance today, of course, is the application and the use of fraudulent I.D. by a terrorist. The use of false or stolen identity enhances its chances of success in commission of almost all crimes, especially financial crimes. The identity provides a cloak of anonymity for the subject while the groundwork is laid to commit the crime. This includes the rental of mail post offices boxes, apartments, office spaces, vehicles, and storage lockers, as well as the activation of pagers, cellular telephones and various utility services.

The crucial element in the acceptance of any form of identification is the ability to verify the true identity of the bearer of the identification, which is honestly more important in this post-9/11 world to determine whether an individual is who he purports to be. This is essential in our mission to identify potential terrorists.

The FBI is concerned about the issuance of driver's licenses without adequate verification of identity. The criminal threats and terrorist threats stem from this fact that the driver's license can be a perfect breeder document for establishing a false identity.

Since 9/11, the FBI has investigated numerous incidents where terrorists have utilized false identifications. I have outlined some of those in my written testimony and won't go into detail here other than to mention there are cited five examples of international terrorists who have used false travel documents, false identification to attempt to travel around the world.

And we have also had several examples here in the U.S., one, in particular, that stands out from the 1995 Oklahoma City bombing, Timothy McVeigh, who had nine different forms of identification. A couple of other domestic examples are cited in my written testimony. I won't take time to go into those at this point.

The FBI has implemented, in conjunction with our domestic law enforcement partners, and some in the intelligence community, to address the various fraud schemes being utilized by terrorists to fund their terrorist activities through the use of fraudulent identification. And those, again, are outlined in my written testimony.

One I would like to highlight is a project with the Office of the Inspector General for the Social Security Administration, which is a multi-phase project to identify either fraudulent numbers, fictitious numbers, or those being used by individuals whose name does not match to that. And this is being handled by the Terrorism Fi-

nancing Operations Section, or TFOS, of the FBI Counterterrorism Division.

We are also working on several joint interagency working groups involving bank regulators of the state, local and Federal Government regulatory agencies as part of the financial services industry trying to bring together a two-part national identify theft assistance and investigative referral system.

The law enforcement component will work in conjunction with a victim/witness assistance center to be operated by the financial service industry and will receive complaints, collect, aggregate and analyze data and refer cases to identity task forces nationwide to target terrorists or organized groups perpetrating identify theft.

In conclusion, I want to thank you again for the invitation to be here to speak to you today. One of the keys is the nation's reliance on paper documents, and until we move to some type of standardized biometrics approach, we will be struggling with the same issues we have.

Thank you, Mr. Chairman.

[The statement of Mr. Pistole follows:]

PREPARED STATEMENT OF MR. JOHN S. PISTOLE, FEDERAL BUREAU OF INVESTIGATION ASSISTANT DIRECTOR, COUNTERTERRORISM DIVISION

Good morning Chairman Cox, Ranking Member Turner, and members of the Committee. On behalf of the Federal Bureau of Investigation (FBI), I would like to thank the Committee for affording us the opportunity to participate in this forum and comment on the use of fraudulent identification documents and the implications for homeland security.

As this Committee is well aware, the FBI, along with other federal law enforcement agencies, investigates and prosecutes individuals who use false identities, or the identities of others, to carry out violations of federal criminal law. These violations include bank fraud, credit card fraud, wire fraud, mail fraud, money laundering, bankruptcy fraud, computer crimes, and fugitive cases. When these crimes are carried out using a false or stolen identity, investigation of the offenses becomes much more complicated. The use of a false or stolen identity enhances the chances of success in the commission of almost all financial crimes. The identity provides a cloak of anonymity for the subject, while the groundwork is laid to carry out the crime. This includes the rental of mail drops, post office boxes, apartments, office space, vehicles, and storage lockers, as well as the activation of pagers, cellular telephones, and various utility services.

Identity theft, and the use of false identities, is not new to law enforcement. For decades fugitives have changed identities to avoid capture and check forgers have assumed the identity of others to negotiate stolen or counterfeit checks. What is new today is the pervasiveness of the problem. The Federal Bureau of Investigation does not view the use of false identities and identity theft as a separate and distinct crime problem. Rather, it sees this issue as a component of many types of crimes, which we investigate.

Advances in computer hardware and software, along with the growth of the Internet, have significantly increased the role that identity theft and false identities play in crime. For example, the skill and time needed to produce high-quality counterfeit documents has been reduced to the point that nearly anyone can become an expert. Criminals and terrorists are now using the same multimedia software used by professional graphic artists. Today's software allows novices to easily manipulate images and fonts, allowing them to produce high-quality counterfeit documents. The tremendous growth of the Internet, the access it provides to such an immense audience and the anonymity it allows users result in otherwise traditional fraud schemes becoming magnified when the Internet is utilized as part of the scheme. This is particularly true with identity theft related crimes. Computer intrusions into the databases of credit card companies, financial institutions, on-line businesses, etc. to obtain credit card or other identification information for individuals have launched countless identity theft related crimes.

The impact is greater than just the loss of money or property. As the victims of identity theft well know, it is a particularly invasive crime that causes immeas-

urable damage to the victim's good name and reputation in the community; damage that is not easily remedied.

Today, the threat is made graver by the fact that terrorists can utilize identity theft as well as Social Security Number fraud to enable them to obtain such things as cover employment and access to secure locations. These and similar means can be utilized by terrorists to obtain Driver's Licenses, and bank and credit card accounts through which terrorism financing is facilitated. Terrorists and terrorist groups require funding to perpetrate their terrorist agendas. The methods used to finance terrorism range from the highly sophisticated to the most basic. There is virtually no financing method that has not at some level been exploited by these groups. Identity theft is a key catalyst fueling many of these methods.

The crucial element in the acceptance of any form of identification is the ability to verify the actual true identity of the bearer of the identification. In today's post-9/11 world, this element is all the more important because, in order to protect the American people, we must be able to determine whether an individual is who they purport to be. This is essential in our mission to identify potential terrorists, locate their means of financial support, and prevent acts of terrorism from occurring.

Foreign nationals who are present in the U.S. legally have the ability to use various alternative forms of identification, most notably a passport, for the purposes of opening bank accounts, gaining access to federal facilities, boarding airplanes, and obtaining a state driver's license. In addition, foreign nationals who are present in the United States, either legally or illegally, have the ability to obtain a passport from their own country's embassy or consular office.

The FBI is concerned about the issuance of driver's licenses by states without adequate verification of identity. The criminal threats stem from the fact that the driver's license can be a perfect ″breeder″ document for establishing a false identity. The use of a false identity can facilitate a variety of crimes, from money laundering to check fraud. And of course, the false identity serves to conceal a criminal who is already being sought by law enforcement. Such false identities are particularly useful to facilitate the crime of money laundering, as the criminal is able to establish one or more bank accounts under completely fictitious names. Accounts based upon such fraudulent premises greatly hamper money-laundering investigations once the criminal activity is discovered. As the Committee is well aware, the FBI is particularly concerned about fraudulent financial transactions in the post 9/11 environment, given the fact that foreign terrorists often rely on money transferred from within the United States.

The ability of an individual to create a well-documented, but fictitious, identity in the United States provides an opportunity for terrorists to move freely within the United States without triggering name-based watch lists that are disseminated to federal, state and local police officers. It also allows them to board planes without revealing their true identity and in some cases purchase firearms. All of these threats are in addition to the transfer of terrorist funds, mentioned earlier.

The FBI, since 9/11/2001, has investigated numerous incidents where terrorists have utilized false or stolen identifications. For example, an Al-Qa'ida terrorist cell in Spain used stolen credit cards in fictitious sales scams and for numerous other purchases for the cell. They kept purchases below amounts where identification would be presented. They also used stolen telephone and credit cards for communications back to Pakistan, Afghanistan, Lebanon, and other countries. Extensive use of false passports and travel documents were used to open bank accounts where money for the mujahadin movement was sent to and from countries such as Pakistan and Afghanistan.

While the 9/11 hijackers did not utilize fraudulent identification, they did obtain US identification cards in their true names. These are ″legitimate″ identification cards, but they are not issued by any state or federal agency. Some of the vendors the hijackers received these cards from were involved in fraudulent identification cases--they were subsequently charged and arrested. In Virginia, some of the hijackers used a loophole to apply for, and receive, legitimate state identification cards and Driver's Licenses.

Investigation and interviews of detainees have included the following instances of fraudulent documents and use of false identification related to terrorism matters: (1) A Pakistani detainee who served as a doctor and guard for the Taliban was detained at JFK for attempting to enter the US on a forged passport; (2) An Iraqi detainee purchased a false Moroccan passport for approximately $150.00 in US currency, and used it to enter Turkey where he was arrested; (3) An Algerian detainee requested asylum in Canada after entering that country on a false passport; (4) A Yemeni detainee acquired a false Yemeni passport and was able to get a Pakistani visa; and (5) An Algerian detainee obtained a French passport in an alias name and

used it to travel to London. The cost for this false passport was 3,000 French Francs (about $530 US, according to the Council of Economic Advisors).

The FBI has seen other examples of document and identification fraud in our investigations related to terrorism, to include: (1) the April 2003 arrest of William Joseph Krar in Tyler, Texas. Krar is the subject of a fraudulent identification matter, which was initiated in August 2002 based upon information developed following the delivery of a package of fake identification cards to the wrong address. The package, which contained numerous false identifications, had been mailed from Krar in Tyler, Texas to an individual in New Jersey, an admitted member of the New Jersey Militia. The identities included a Defense Intelligence Agency identification, a United Nations Observer Badge and a Federal concealed weapons permit; (2) former Top Ten Most Wanted fugitive Clayton Lee Waagner was found to have in his possession fraudulent US Marshal's badges and a significant amount of equipment for making fraudulent identification cards, in addition to bomb making materials and large amounts of currency; and (3) The investigation of the bombing of the Oklahoma City Murrah Federal Building was a collaborative effort between by the FBI and many other federal, state, and local law enforcement agencies. The evidence developed and presented in court led to the convictions of both Timothy McVeigh and Terry Nichols by two separate juries of their peers. McVeigh and Nichols, like others planning to commit criminal acts, utilized aliases. McVeigh was also known to utilize fraudulent identification.

The FBI has implemented a number of initiatives to address the various fraud schemes being utilized by terrorists to fund their terrorist activities. One involves targeting fraud schemes being committed by loosely organized groups to conduct criminal activity with a nexus to terrorist financing. The FBI has identified a number of such groups made up of members of varying ethnic backgrounds, which are engaged in widespread fraud activity. Members of these groups may not themselves be terrorists, but proceeds from their criminal fraud schemes have directly or indirectly been used to fund terrorist activity and/or terrorist groups. By way of example, the terrorist groups have siphoned off portions of proceeds being sent back to the country from which members of the particular group emigrated. We believe that targeting this type of activity and pursuing the links to terrorist financing will likely result in the identification and dismantlement of previously unknown terrorist cells. Prior to 9/11, this type of terrorist financing often avoided law enforcement scrutiny. No longer. The FBI will leave no stone unturned in our mission to cut off the financial lifeblood of terrorists.

Another initiative has been the development of a multi-phase project that seeks to identify potential terrorist related individuals through Social Security Number misusage analysis. The Terrorist Financing Operations Section of the FBI works with the Social Security Administration's Office of the Inspector General for SSN verification. Once the validity or non-validity of the number has been established, investigators look for misuse of the SSNs by checking immigration records, Department of Motor Vehicles records, and other military, government and fee-based data sources. Incidents of suspect SSN misusage are then separated according to type. Predicated investigative packages are then forwarded to the appropriate investigative and prosecutive entity for follow-up.

The events of 9/11 forever changed our world. As unpleasant as it may be, we must face the realities of our current world as they relate to protecting the people of the United States. This requires continual vigilance, particularly when it comes to being able to detect and deter those who might abuse the system to directly cause harm, or those who might aid and abet the financing of terrorist operations.

I again want to thank you for your invitation to speak here today, and on behalf of the FBI, look forward to working with you on this very important topic.

Chairman COX. Thank you very much for your statement.

Next, we have with us the United States Attorneys, both for the Eastern District of Virginia and the District of Columbia, who are exceptionally familiar with the problems that we are discussing in the nation's capital area.

Welcome to both of you.

Mr. McNulty, you are recognized for your statement.

STATEMENT OF MR. PAUL J. McNULTY, UNITED STATES ATTORNEY, EASTERN DISTRICT OF VIRGINIA DEPARTMENT OF JUSTICE

Mr. MCNULTY. Thank you, Mr. Chairman and Mr. Turner. It is great to be back in the House.

As I look at the cases that we are working on in my office, the investigations, the prosecutions, I think it is clear that terrorists need three things to operate: first, they need to conceal or establish their identity; second, they need money to operate and; third, they need an opportunity to strike.

So if we are going to prevent terrorism, if we are going to disrupt, if we are going to try to be proactive rather than just investigate cases after they occur, we need to focus resources on those three areas. And that has to do with, again, strengthening the integrity of our identification system, making sure that funding doesn't flow to the terrorists or scams by credit card bust-out schemes or other things aren't used to support terrorists here.

And then third, we have to harden our targets. We have to make sure that our airports, our military bases or ports are not vulnerable and an opportunity to strike is not there. That is how we have kind of organized our efforts in the Eastern District of Virginia on the prevention side.

As has already been said, identification fraud and document fraud is an enormous problem. Identification is on sale in the streets of America. They can be purchased by criminals, terrorists, anybody that wants to pose as someone else.

Thousands upon thousands of government identification documents are produced or sold by fraud every month, including state driver's licenses, identification cards, social security, green cards, birth certificates, and U.S. passports. Some of them are counterfeit; others are genuine government documents that have been obtained through corruption or false statements.

All of them enable the holders to conceal their true identity, or, as in the case of the hijackers to establish themselves in a way that gives them more legitimacy.

For some reason, Virginia has become a hub of identification and document fraud. We have more cases than we could ever hope to prosecute; the problem is so widespread. We have had a number of big cases recently.

We recently prosecuted an individual who was responsible for acquiring labor certificates, certificates issued from the Department of Labor that he would turn around and sell to individuals for anywhere from $7,000 to $20,000 per application. He sold over 2,700 fraudulent certificates. This individual was convicted on 57 accounts of conspiracy, labor certificate fraud, immigration fraud, and money laundering.

We had another case involving the Virginia Department of Motor Vehicles and driver's license corruption and fraud. And we had recently a large case where we prosecuted someone for selling over one thousand per month false Virginia driver's license and identification cards.

Recently we arrested and are in the process of prosecuting another scheme involving labor certification, and in this case, we have over 150 false applications and the charges there—two of the appli-

cants are anywhere from $10,000 to $50,000 per application. That is just a small sample of the kinds of cases that we are seeing and that we are trying to pursue.

And again, there is a lot of money in this. In the case of Mr. Kooritzky with the nearly three thousand false labor certifications there was more than $6 million seized and forfeited in that case. We found over one million dollars in cash under his bed.

Now, the question is, "What are we doing about this," as far as trying to get at the problem on a large-scale basis. And in the Eastern District of Virginia we have formed a task force, an Immigration and Visa Fraud Task Force, to try to bring together the resources from many different agencies, because the problem is so great, that no one agency has the authority or the resources to take on the problem.

And in my testimony I have all of the agencies who are involved in our task force. We meet about once a month in the office and we identify the cases that are the most important ones to pursue and we try to pull together the combined efforts to be most effective.

And so, I am happy to discuss in more detail this task force approach, which I think, is a model for how we can be effective in this area across the country.

And I thank you for your time.

[The statement of Mr. McNulty follows:]

PREPARED STATEMENT OF MR. PAUL J. MCNULTY, UNITED STATES ATTORNEY EASTERN DISTRICT OF VIRGINIA

Mr. Chairman and Members of the Committee: As the United States Attorney for the Eastern District of Virginia, I am privileged to serve the public and to lead a talented staff in a district on the front lines of the war against terrorism. It is also my privilege to appear before you today to discuss the significant problem identification document fraud poses for our national security.

I. Scope of the Problem

Identification document fraud is a serious, national problem. Simply put, identities are for sale on America's streets—to criminals, to terrorists, to anyone who wants to pose as someone else. Thousands upon thousands of government identification documents are produced or sold by fraud every month, including state drivers licenses and identification cards, Social Security cards, green cards, birth certificates, and U.S. passports. Some of these documents are counterfeit; others are genuine government documents that have been obtained through corruption or false statements. All of them enable holders to conceal their real identity and where they really come from.

Unfortunately, identification document fraud has become widespread in Northern Virginia. People from all over the United States come here to obtain fraudulent identification. In just the past three years, my office has investigated and prosecuted a string of identification document frauds of a size we rarely, if ever, saw before. To give a few examples:

• Samuel G. Kooritzky of Vienna, Virginia, was convicted in March on 57 counts of conspiracy, labor certification fraud, immigration fraud and money laundering. Mr. Kooritzky, who practiced law in Virginia, Maryland and the District of Columbia, filed false applications for alien employment certificates with the U.S. Department of Labor. These certificates allow immigrants to apply for a green card to live and work in the United States. Mr. Kooritzky filed over 2,700 fraudulent applications within an 18 month time frame. He charged between $7,000 and $20,000 per application.

• Jennifer Wrenn, a notary public and owner of a realty company in Northern Virginia, was convicted in August 2001 for selling fraudulent Virginia drivers licenses and identification cards to illegal immigrants from all over the United States. At its height, this operation sold fraudulent documents to over 1,000 aliens a month. After a year-long investigation, Ms. Wrenn and thirteen of her associates, including a lawyer, were convicted of various crimes, including identification document fraud,

money laundering, and encouraging illegal immigration. Several of the defendants, including Ms. Wrenn, her husband, and the lawyer, were sent to prison; many of the rest were deported.

• Most recently, Steven Y. Lee, Jordan N. Baker, and Byung Chul Kim were charged in August with filing fraudulent applications for alien employment certifications with the United States Department of Labor. Lee and Baker are alleged to have prepared and submitted applications they knew contained false information and forgeries on behalf of many different employers and immigrants. In particular, they are suspected of colluding with local employers—one of whom was Kim—to file applications seeking immigrant workers for jobs the employers did not have and did not intend to fill. Lee and Baker sold these applications to Korean immigrants who would then use the approved applications to obtain employment authorizations but would never work for the sponsoring employer. Lee and Baker charged the illegal immigrants between $10,000 and $50,000 per application, a portion of which fee Lee and Baker paid as a kickback to the cooperating employer. Of the 150 applications known to have been submitted by these defendants, the vast majority are believed to be fraudulent.

• Our Office's prosecution of Ousmane Sow and Aboubakar Doumbia for Social Security fraud illustrates how easily Social Security cards are obtained by fraud and how widespread the abuse is. Sow and Doumbia were caught at Reagan National Airport in transit from New York to Miami. They were traveling on tickets paid for with stolen credit cards and were found to be carrying a dozen foreign passports and two dozen stolen immigration forms. Both men were charged with immigration fraud and pled guilty prior to trial. Interestingly, both had fraudulent Virginia identification cards even though they lived in New York.

One of the two men agreed to cooperate with the government and revealed the purpose of their trip to Miami. He and his accomplice were part of a West African criminal syndicate based in New York City. This syndicate specialized in the fraudulent procurement of Social Security cards and, to a lesser extent, the fraudulent procurement of Virginia drivers licenses and identification cards. Members of the syndicate repeatedly traveled from New York to major cities in the United States on tickets paid for with stolen credit cards. The purpose of the trips was to apply for Social Security cards by fraud at the Social Security Administration offices in each city. At each office, the members of the syndicate would apply for a card using a passport and an INS form.[1] The members of the syndicate altered the passports by substituting their own photographs so that they could apply in person for a Social Security card in the name of one of the syndicate's clients (to whom the passport actually belonged). They further placed doctored INS forms in the client's passport to make it appear that they, the applicants, were lawfully in the United States and had the right to work. In fact, their clients were illegal immigrants in New York and New Jersey who paid the syndicate between $700 and $1,500 for a Social Security card. Members of the syndicate obtained well over a thousand fraudulent Social Security cards.

• airport Security Task Force: After September 11, 2001, the Department of Transportation (DOT) became concerned that large numbers of employees at National and Dulles airports had obtained their airport secure area access badges by fraud or misrepresentation. A task force was convened to investigate all 28,000 badge holders. In the end, approximately 120 of them were charged with various crimes, including making false statements, Social Security fraud, and immigration fraud. Another twenty badge holders were arrested by INS (now part of DHS's Bureau of Immigrations and Customs Enforcement) on administrative charges.

These cases, and many others like them, demonstrate that identification document fraud is pervasive. If a person is willing to pay the price, he or she can obtain fraudulent identification for any purpose, no questions asked. These cases also reveal that identification document fraud is big business. Kooritzky made no less than $6,300,000 in the space of eighteen months, including $1,000,000 in cash seized from a suitcase under a co-conspirators's bed. It is also easy: many defendants have told us that they bought their Social Security cards and green cards on the street for as little as $50.

II. Relevance to Homeland Security

Identification document fraud directly undermines our homeland security. It also creates huge holes in our immigration and naturalization controls; it enables terrorists to enter and remain in our country; and it facilitates crime—crime such as credit card fraud, mortgage fraud, and bank fraud, the proceeds of which can be used to support sleeper cells or finance large-scale terrorist attacks in this country.

[1] The form used was an INS form I–94, which is a record of authorized entry.

Fraud involving state drivers licenses is of a particular concern. Drivers licenses are a primary source of identification and a mainstay of daily life in this country. With a drivers license, you may drive a car, board an airplane, and purchase a handgun. You may open bank accounts, buy alcohol, and obtain credit cards. In addition, although a driver's license is not evidence of lawful residence in the United States, it may be perceived as such. In short, the integrity of state drivers licenses is critical to our commerce and our national security.

Given the importance of drivers licenses and other government identification documents, we cannot afford to ignore serious identification fraud. Widespread fraud in government programs is simply bad government and should be vigorously fought as a matter of principle. No one benefits when state and federal programs are routinely abused. In addition, identification document fraud undermines public confidence in government, particularly our ability to protect the national security. We cannot restore public trust in our immigration and border controls if fraudulent green cards, drivers licenses, and Social Security cards remain available to anyone with cash to buy them. This sort of fraud presents terrorists and other serious criminals with an easy way to gain entry to the United States.

Most important, identification document fraud facilitates terrorism. Seven of the September 11th hijackers[2] obtained genuine Virginia drivers licenses by submitting false proof of Virginia residency to the DMV.[3] One of the seven was involved in the failed attempt to fly Flight 93 into a target here in the Washington, D.C., area; two were aboard the airplanes that crashed into the World Trade Center; and four were aboard Flight 77 when it was flown into the Pentagon. None of the seven lived in Virginia. Rather, they made a special trip to Virginia, because they knew they could get a genuine drivers license in one day for approximately $100 in cash with no questions asked. And although we will never know for sure, we strongly suspect that these seven hijackers intentionally used their Virginia drivers licenses to board the flights they hijacked to avoid the scrutiny a foreign passport would bring.

II. Challenges Law Enforcement Faces in Combating the Problem

The Administration is working to address identity theft on a collaborative basis. The Departments of Justice and Homeland Security, the Federal Trade Commission, the U.S. Postal Inspection Service, and other agencies are all working hard to combat this problem.

Unfortunately, however, as the last few years have shown, immigration and identification fraud is flourishing in this country. First, there are simply too many large-scale frauds to investigate all of them. Second, we have recognized the need for improved coordination among the agencies with jurisdiction to investigate document fraud offenses. Many different federal and state agencies have authority to investigate these crimes, but they rarely coordinate their efforts beyond a given case.

There are a number of additional steps we can take to fight identification document fraud more effectively and to improve our homeland security. First, we can ensure that federal law enforcement agencies have the authority to investigate all forms of identification document fraud, from Social Security cards to employment authorizations to airport security badges. Together with state law enforcement, federal agencies could pursue a truly national effort to combat identification document fraud.

Second, we must improve coordination among the many federal and state agencies with authority to investigate the various forms of identification document fraud. Given the extent of the fraud we face, no one federal agency can be expected to tackle the problem alone. As a preliminary matter, the number and scale of the frauds are simply too much for one agency. Furthermore, most of the large frauds involve multiple government programs and cut across agency jurisdictions and state lines. For example, we often find that the same document vendor who sells fraudulent state drivers licenses also sells fraudulent Social Security cards and green cards. In such a case, it is essential that the investigation involve agents from the state motor

---

[2] The seven were Hani Hanjour, Khalid Almihdhar, Majed Moqed, Salem Alhazmi, Abdulaziz Alomari, Ahmed Alghamdi, and Ziad Jarrah.

[3] Since September 11, 2001, this Office has prosecuted four individuals who helped the hijackers complete fraudulent forms and submit them to the Virginia Department of Motor Vehicles ("DMV"). All four were charged with and pled guilty to identification document fraud, in violation of 18 U.S.C. § 1028. In addition, this Office has used 18 U.S.C. § 1028 to prosecute several people who came to our attention through the 9/11 investigation, either due to their contacts with the hijackers or because of their presence near Dulles airport on September 11th with flight manuals. We also prosecuted two men who ran a checkpoint at the Pentagon in a tow truck in February of this year. In each of these cases, the defendant submitted false information to the Virginia DMV to obtain a Virginia identification card or license for himself or another by fraud.

vehicle agency, the Social Security Administration's Office of the Inspector General, and the Department of Homeland Security.

Third, we should review our procedures that govern the issuance of identification documents to ensure they are effective. Our prosecutions of large immigration and identification document frauds have revealed that the underlying regulatory and adjudicatory processes invite much of the abuse. There are too many unintended loopholes and too few efforts to identify and deter fraudulent applications. In short, our own procedures may sometimes make it easy for the unscrupulous to defraud the government. As a result, we must place as much emphasis on reviewing the underlying programs as we do on prosecuting crimes against those programs.

To be effective, the steps I have just outlined will need to be pursued at a national level, but the same principles work at the local level. In my district, for example, we quickly realized that identification document fraud was one of the most significant threats to our homeland security in the wake of September 11. We also realized that the conventional model of investigating and prosecuting these cases was not capable of dealing with the problem. In response, we created the Immigration and Visa Task Force early this year specifically to address immigration and identification document fraud.

The purpose of the task force is to create a standing group of agents and prosecutors to identify, investigate, and prosecute large immigration, visa, and identification document frauds. The primary aims of the task force are (1) to restore integrity to the nation's immigration and identification document controls and (2) to prevent terrorists and criminals from entering and residing in the United States.

The basic idea behind the task force is to bring agents from the various agencies with the relevant enforcement powers together with prosecutors to target and prosecute the bigger frauds in our area for maximum effect. These frauds require substantial resources and time, but provide great deterrence because of the publicity and length of sentences they generate. The task force also pursues forfeiture as a further deterrent. This too requires a good deal of investigation, but is well worth the effort (e.g., the government obtained $6.3 million in forfeiture in the Kooritzky case).

The task force meets approximately once a month at the United States Attorney's Office and is chaired by an Assistant United States Attorney. At each meeting, the members of the task force review the status of existing cases, examine new leads, and discuss practices or problems that deserve investigation. The members of the task force are

(1) United States Attorney's Office;
(2) Department of Homeland Security—U.S. Immigration and Customs Enforcement;
(3) Department of Homeland Security—Secret Service;
(4) Department of Homeland Security—U.S. Citizenship and Immigration Services ;
(5) DOJ—FBI;
(6) DOJ—Office of Inspector General;
(7) Department of Labor;
(8) Department of State;
(9) Social Security Administration, Office of the Inspector General;
(10) IRS;
(11) US Postal Inspection Service;
(12) Virginia DMV;
(13) Fairfax County Police Department; and,
(14) Metropolitan Washington Area Airport Police.

The participating agencies have worked well together, and the task force has already brought two large frauds to a close.

That concludes my testimony, Mr. Chairman. I am pleased to answer any question you may have.

Chairman COX. Thank you very much.

Roscoe C. Howard, Jr. is the United States attorney for the District of Columbia, also exceptionally familiar with the things that were described by the National Capital area. Thank you very much for being here.

I know, in fact, that your work has come to the attention of Representative Eleanor Holmes Norton, and is one of the reasons that we are having this hearing. So I appreciate your being here today.

STATEMENT OF MR. ROSCOE HOWARD, JR., U.S. ATTORNEY FOR THE DISTRICT OF COLUMBIA

Mr. HOWARD. I appreciate the opportunity to come and testify. And I am also thanking members of the committee, and I would especially like to thank Representative Eleanor Holmes Norton, not only for her leadership, but focusing all of our efforts on this problem.

D.C. is like a lot of cities where there is a high concentration of illegal immigrants. The business of counterfeit identification documents just thrives here.

Since 1998, our office has been working aggressively with a number of law enforcement offices. The Bureau of Immigration and Customs Enforcement, MPD, the FBI, Social Security Administration, the U.S. Postal Service, IRS, the Secret Service, the Diplomatic Security Service, out of the Department of State and the Department of Labor.

We get together to try to figure out exactly how we are going to fight this menace posed by the manufacturing and distribution of false and fraudulent documents. Now what we have done is our office has conducted four major operations focusing primarily on the Adams Morgan section of the city, where we probably have our most diverse population.

These investigations have resulted in dozens of convictions of manufacturers and distributors of false documents. One of our most recent that you have heard referred to, Operation Card Shark, was actually in response to complaints from the community. These gentlemen that were operating, women and gentlemen, was basically an open-air market up in the Northwest section. We used Federal agents and MPD agents to make observations, to secure warrants and then we executed those warrants.

And what we recovered were just a number of blank documents for making green cards and social security cards, as well as equipment for laminating. We also were able to identify the kingpin, a gentleman by the name of Soloman Gonzalez–Gonzalez. We identified him as the owner of the equipment and the owner of the mills. What we do know is a lot of the documents that he was getting were actually being imported from California, where they were made. We ended up with a number of sentences that ranged from about 27 months up to Mr. Gonzalez's 52 months that he received on July 15th.

In another recent case, Calvin McCants, the owner of a false document-making factory in the 2100 block of P Street N.W. recently entered a guilty plea to possession of false document-making implements. And depending on the court's decision on the monetary loss, Mr. McCants is facing somewhere between 27 months and 63 months and he will be sentenced later this month in October.

But in executing search warrants, while what we found in the defendants' offices and storage facilities in Washington and throughout this area were a wide variety of document-making equipment, including blank and finished passports, military identification, driver's licenses from almost all 50 states, birth certificates, access devices, other official documentation and pamphlets such as "New I.D.s in America" and "How to Make Driver's Licenses and Other I.D.s." These are just a couple of examples of

what our office is doing, as many of the offices, including Mr. McNulty's, are doing across the country.

This year alone, we have initiated about 40 false document cases involving a huge number of defendants. Now as we address these—when we first started addressing this well before 9/11, our office was addressing them, they started off as identity and theft issues, but after 9/11, it is clear that they also become critical to looking at the terrorism issue.

Often in terrorism what we are doing is looking for a needle in a haystack, but that is what our jobs are and that is what we intend to. Our efforts will continue, we will work with law enforcement to get this, but one thing that is clear, as I go through these cases, is that law enforcement alone cannot accomplish of reducing the probability that there could be another terrorist attack.

I think that we as a government need to think constructively about not only how we design our identification documents, but how we issue those identification documents. And in addition, our office and certainly the Department of Justice is keenly interested in exploring legislative improvements in this area. For example, the department strongly supports H.R. 1731, the Identity Theft Penalty Enhancement Act, which is pending before the Judiciary Committee.

I want to again, Mr. Chairman, thank you for the opportunity to testify today, and as everybody else, I will be glad to answer questions.

[The statement of Mr. Howard follows:]

PREPARED STATEMENT OF THE HONORABLE ROSCOE C. HOWARD, JR.

Mr. Chairman, Members of the Committee, I appreciate the opportunity testify today on the threat to national security posed by false and fraudulent identification documents. I would like to express my appreciation to Representative Eleanor Holmes Norton, who has focused attention on this important issue and continues to seek resources to help combat this problem at the local level.

The District of Columbia is a diverse city of over 570,000 residents. We have people from countries all over the world who bring a rich diversity to our communities and neighborhoods. Many of our residents emigrate here legally, following in the footsteps of our forefathers. However, many others, in the District and across the country, are not here lawfully or have allowed their legal status to lapse. In cities where there is a high concentration of illegal immigrants, the business of counterfeit identification documents thrives. The District of Columbia is no exception. Illegal "document mills" provide a variety of identification documents to their customers, including green cards, social security cards, driver's licenses, and passports.

Since 1998, the United States Attorney's Office for the District of Columbia has been working aggressively with our local and federal law enforcement partners to combat the menace posed by the manufacture and distribution of false and fraudulent identification documents. We have conducted four major operations focusing primarily on document mills in the Adams Morgan section of the city, which have resulted in the conviction of dozens of manufacturers and distributors of false alien registration cards and social security cards. The most recent of these is Operation Card Shark,[1] which resulted in the sentencing on July 15 of kingpin Salomon Gonzalez-Gonzalez, (aka Angel Marques, aka El Virus) to an aggregate of 52 months in prison for conspiracy to distribute false documents, distribution of false documents, possession of document-making implements, possession with intent to distribute more than five documents, and re-entering the country illegally after deportation. Aspects of this investigation are on-going.

Operation Card Shark started in response to complaints from the community about document vendors in the area of Columbia Road, N.W. between 16th and 18th

[1] The earlier operations were named Southside (1998–2000), Operation Mica Maker (2000–2001) Identity Crisise (2000–2001). "Mica" is a Spanish word for a government-issued identification card.

Streets. Agents from the Bureau of Immigration and Customs Enforcement (BICE) conducted surveillance, obtained search warrants, and seized hundreds of blank documents as well as equipment for making false cards. Forensic examination of these items revealed Gonzalez-Gonzalez's fingerprints at several locations. Further investigation revealed that Gonzalez-Gonzalez purchased and owned the equipment in the document mills, hired other illegal aliens to sell counterfeit documents, and paid them and the workers in the mills based on the number of sales. Consequently, he was regarded as the boss and was sentenced accordingly.[2]

In another recent case, Calvin McCants, the owner of a false document-making factory in the 2100 block of P Street, N.W., entered a guilty plea to possession of false document-making implements. Depending on the court's decision on the monetary loss attributable to the defendant, he could face up to 27 months or 63 months when he is sentenced later this month. The defendant's plea followed the execution of three search warrants at defendant's offices and storage facilities. In the first, the U.S. Secret Service's Financial Crimes Task Force found: a scanner; a lamination machine and laminated sheets; a corner rounder (for cutting corners off cards); a color laser-printer; a cutting board; metal seal presses (used to emboss raised seals on official documents for several jurisdictions, including the District of Columbia); computers; computer discs containing templates for official identification documents (such as passports, military identifications, driver's licenses, and birth certificates); driver's licenses from several states and the District; access devices in the same names as the driver's licenses; and other finished and unfinished identification documents. The second and third searches, at different locations, netted a number of documents bearing McCant's photograph but other names, along with other equipment and documents. Pamphlets entitled "New ID's in America," "How to make driver's licenses and other ID's on your home computer," and "2000 ID checking guide" were also found.

These are two examples of the efforts that we have been undertaking to curb trafficking in false and fraudulent identification documents. Other initiatives include prosecuting those who commit passport and visa fraud, arrange sham marriages for immigration purposes, obtain false labor certificates, and use false social security numbers on employment documents. In 2003, we have had over 40 cases of this nature involving a larger number of defendants. We have worked closely with BICE and its predecessor, the Immigration and Naturalization Service, the Metropolitan Police Department, the Federal Bureau of Investigation, the Social Security Administration, the U.S. Postal Inspection Service, the Internal Revenue Service, the United States Secret Service, and the Departments of State and Labor.

What we used to address only as immigration or identity theft issues has become critically more important as a terrorism issue. Those who are bent on undermining our society and destroying our government are adept at using false and fraudulent identification documents that allow them to move easily across borders and within our country.

So the efforts we have undertaken—and will continue to undertake—to combat counterfeit identification documents need to be doubled and re-doubled. Law enforcement alone, however, cannot accomplish the goal of reducing the probability that terrorists can obtain and use false identification documents to advance their cause. We need to think constructively about how we design and issue identification documents that are less susceptible to counterfeiting. We have made changes in our currency in recent years for this purpose, and we may need to make changes in other official documents. It is a more complicated task, I know.

The federal government has a leadership role to play in developing and promoting new technology and in assisting the states and the District of Columbia to use such technology to reduce the probability that identification documents can be created in illegal document mills.

In addition, we are very interested in exploring legislative improvements in this area. For example, the Department strongly supports H.R. 1731, the "Identity Theft Penalty Enhancement Act," which is pending in the Judiciary Committee. I note that the Senate passed an identical bill, S. 153, by unanimous vote on March 19, 2003.

Thank you for the opportunity to testify today. I would be pleased to answer any questions you might have.

Chairman COX. Thank you very much for that testimony.

---

[2] Six other members of the conspiracy were sentenced to periods of incarceration of up to 27 months. Related cases against eight co-conspirators are pending.

Our next witness is Joseph R. Carico, who is the Chief Deputy Attorney General from the Commonwealth of Virginia.

Thank you very much for joining us, and as I said in our opening statement, thank you, the attorney general, the governor and the legislature of Virginia for moving so swiftly to correct the problems that we identified.

STATEMENT OF MR. JOSEPH CARICO, CHIEF DEPUTY ATTORNEY GENERAL COMMONWEALTH OF VIRGINIA

Mr. CARICO. Thank you, Mr. Chairman, Mr. Ranking Member, members of the committee, thank you for allowing us to be here today.

I represent the Attorney General of Virginia, Jerry Kilgore, and he sends his greetings and thanks for letting our office be represented as you discuss these important security and safety concerns of all Americans.

The hijackers of 9/11 had many different things in common; one of the main things is that they had an intense hatred for America and everything that we stand for. Seven of those terrorists as has been pointed out today also shared another characteristic; seven of those terrorists had Virginia driver's licenses or identification.

It is a sad fact that our Commonwealth had become known in the terrorist community as an easy place to obtain state driver's licenses or state identification cards. And this is a lapse in security in Virginia that we sought to rectify.

A valid driver's license, as you all know, is a passport to all sorts of places and behavior, including of course, boarding airplanes. Attorney General Kilgore recognized that fact and set out to rectify that with members of our General Assembly and they sought legislation that tightens the controls on the issuance of Virginia driver's licenses. Now, in order to obtain a Virginia driver's license, a person must show proof that they are either a United States citizen or that they have legal presence in this country.

There are provisions that have been made for individuals who have immigration situations pending. United States citizens, green card holders, resident aliens or others, such as individuals who sought political or religious asylum may still obtain Virginia driver's licenses. They must simply document their lawful status now.

In addition, if a person is in this country with a legal immigration document, his driver's license issued will expire on the same day as the applicant's authorization to be in the United States. We recognize that it made no sense at all to issue a Virginia driver's license for 5 years if that person's authorization to be in this country was for only 2 years.

The new law also says that if you illegally obtained a driver's license then you are guilty of a Class Six felony, which in our state, brings a prison term of 5 years and a $2500 fine. Of course, identity must also be proven still in Virginia to receive a Virginia driver's license.

Every 16 year old who goes and gets their license now has to still prove that they are who they say they are. We have experienced firsthand, in Virginia, what could happen when people are not held to high standards and required to show proof of identity and legal presence in this country.

Other states may have taken different actions, but in Virginia we suffered one of those attacks on that dark day in September.

We are proud to be working with Congressman Eric Cantor of the 7th District of Virginia. He has been carrying legislation that is very similar to ours here in Congress, and clearly recognizes the public's safety concerns that we all share.

On another front of identity theft, Attorney General Kilgore passed another law, known as the Identity Theft Protection Act which cracks down on the crime of identity theft.

Now there are also the financial costs associated with the crime of identity theft, but in the worst cases of identity theft people are arrested for crimes committed by others who have stolen their identities. In drafting the legislation we started a state-wide Identity Theft Task Force and the U.S. Attorney Paul McNulty was a member of that task force.

One of the worst stories we heard was from a Virginia resident from Southeast Virginia named Angel Gonzalez, Jr. Mr. Gonzalez had his identity stolen by an illegal immigrant who then went on a multi-state crime spree committing crimes in his name; his nightmare culminating when he was arrested in front of his children for crimes that he did not commit.

General Kilgore and the General Assembly sought to rectify this and they created Identity Theft Passport Program, which I can go into further if I am asked about that by any of the members of the committee. The law also makes it a crime to steal an identity of a dead person or to impersonate a law enforcement officer for the purpose of stealing an identity. The law also requires that credit bureaus take notice that someone who was a victim of identity theft has filed a report with the police.

Finally, and importantly, the legislation limits the availability of social security numbers on state documents in a variety of ways, including removing the numbers from state employee I.D. cards, or student I.D. cards, and removing the numbers from the outside of state mailings like tax forms. It also allows the clerks of our circuit courts to refuse accept documents for public recordation that unnecessarily contain social security numbers.

In these ways we can better protect our consumers, provide greater security and go after the criminals who would commit these crimes. Now, would it have changed the events of 9/11 if we had had these laws in place then? We have no way to know that; we will never know that. But we do know that we would have now made it harder and more difficult for those to board airplanes and turn them into guided missiles.

We are pleased the Virginia General Assembly sought to pass these pieces of legislation and we believe we have made our driver's licenses more secure and building greater protection against the security threat of identity theft.

Thank you, Mr. Chairman, for allowing me to be here today.

[The statement of Mr. Carico follows:]

PREPARED STATEMENT OF MR. JOSEPH R. CARICO

Good morning, Mr. Chairman. Mr. Ranking Member. Members of the Committee.

Thank you for allowing me to be here with you this morning. My name is Joseph R. Carico, and I am the Chief Deputy Attorney General for the Commonwealth of Virginia.

I represent the Attorney General of Virginia, Jerry Kilgore. He is unable to be here this afternoon, but sends his greetings and his thanks for allowing our office to be represented as this committee discusses what I believe to be very important ideas for the safety of Americans everywhere.

On the morning of September 11, 2001, nineteen hijackers boarded four airplanes with the intent of flying them into buildings and killing as many Americans as possible. The nineteen men had many things in common, among them an intense hatred for America and everything it stands for.

But seven of the terrorists also shared one other characteristic—hey all possessed Virginia Driver' Licenses or ID cards.

It is a sad fact that our Commonwealth had become known in the terrorist community as a place you could go to easily obtain a valid driver' license or official state Identification card as a foreign national.

This was a lapse in security that we in Virginia vowed we would never allow to happen again.

A valid driver' license is a passport to all sorts of places and behaviors—including, of course, boarding airplanes.

Attorney General Kilgore recognized this fact and set out to do something about it. With two members of the Virginia General Assembly as patrons—Senator Jay O'Brien of Fairfax and Delegate Dave Albo of Springfield—General Kilgore sponsored legislation that tightens the controls on the issuance of Virginia driver's licenses.

Now, in order to obtain a driver's license, a person must provide appropriate documentation that he is either a United States citizen, or is otherwise legally present in this country. There are provisions made for those individuals who have immigration situations pending, such as in the case of someone with a pending application for asylum or protected status.

United States citizens, green card holders, resident aliens, or others, such as individuals who have sought political or religious asylum may all obtain Virginia driver's licenses. They must simply document their lawful status.

In addition, if a person is in this country with a legal immigration document, the driver's license issued will expire on the same day as the applicant's authorization to be in the United States.

We recognized that it made no sense at all to issue driver's licenses that are valid for five years, while the applicant might only be authorized to be in the country for two years.

The new law says that if you illegally obtain a driver's license, you are guilty of a class 6 felony, which carries a penalty of up to five years in prison and a fine of up to $2,500.

The fact of the matter is, identity must be proven routinely at our DMV offices. Every sixteen year old in Virginia, when he gets his first driver's license, must show that he is who he says he is—with a birth certificate or a passport.

We have experienced first hand what can happen when people are not held to high standards and required to show proof of legal presence in this country.

Other states may have taken different action, but in Virginia, we suffered one of the attacks of that dark day more than two years ago.

Simply put, in Virginia, we learned our lesson . . . and we do not feel that it is too much to ask for people to obey the laws of our society before they take advantage of what our society has to offer.

We are proud to have been working with Congressman Eric Cantor of the 7th District of Virginia.

He has been carrying legislation that is very similar to ours here in Congress and clearly recognizes the public safety concerns that we address here today.

Identity Theft

Attorney General Kilgore pushed another new law, known as the Identity Theft Protection Act, which cracks down on the crime of Identity Theft.

There are, of course, financial costs to Identity Theft, as the crime costs merchants, banks, credit card companies and others billions of dollars a year nationwide. Many times victims have spent as many as 400 hours cleaning up the mess in their credit histories. In the worst cases, people were arrested for crimes committed by others who had stolen their identities.

In drafting the legislation, we launched a statewide Identity Theft Task Force. One of the worst stories we heard was from a man in Southeast Virginia named Angel Gonzalez.

Mr. Gonzalez had his identity stolen by an illegal immigrant who then went on a multi-state crime spree—committing crimes in his name.

Mr. Gonzalez's nightmare culminated when he was arrested in front of his children for crimes committed by the Identity thief.

Also in the Tidewater area of Virginia, police have broken up a major crime gang because the Norfolk police made a routine Identity Theft check.

Twenty-three people have no been arrested across the country as part of the crime ring, which is based in Los Angeles, but is spread throughout many states.

These are stories that involve theft, fraud and other crimes. But it is easy to imagine that someone who wanted to slip through the cracks in this country could easily just commandeer someone else's good name.

That's why we created an Identity Theft Passport Program within the Attorney General's Office. These Passports will be issued to people who have documented that they are victims of Identity Theft—to shield them from false arrest and to tell creditors that they did not ring up the bogus charges.

The bill also tightens the laws regarding Identity Theft by making it a crime to steal the identity of a dead person . . . or to impersonate a law enforcement officer for the purpose of stealing an identity. The bill also requires that credit bureaus take note that someone who is a victim has filed a police report.

Finally, the legislation limits the availability of Social Security Numbers on state documents in a variety of ways—including, removing the numbers from state employee IDs or student IDs . . . and removing the numbers from the outside of state mailings, such as tax forms. It also allows the Clerks of Circuit Courts to refuse to accept documents for public recordation that unnecessarily contain Social Security Numbers.

In these ways we can better protect our consumers . . . provide greater security . . . and go after the criminals who would commit these crimes.

Now, if we had had these laws in place two years ago, would we have prevented the events of September 11, 2001?

There is no way to know that.

We know these were determined men . . . determined to kill Americans and strike a blow for their cause.

No, we will never know if we could have completely prevented it. But we do know that we may have made it more difficult for them to board those airplanes and turn them into guided missiles.

I am pleased that the General Assembly saw fit to pass our two pieces legislation. I believe we have made our driver's licenses more secure . . . and built in greater protection against the security threat of Identity Theft.

Thank you for allowing me to be here today.

Chairman COX. Thank you for that testimony.

Mr. Malfi is here representing the General Accounting Office.

In fact, GAO's work in this area which has come to the attention of this committee and to Congress as one of the bases for this hearing. We are very concerned about what GAO has discovered nationwide as part of, if not a 50 state pattern, then a too-often repeating pattern. And we look forward to your testimony.

STATEMENT OF MR. RONALD MALFI, DIRECTOR, OFFICE OF SPECIAL INVESTIGATIONS, GENERAL ACCOUNTING OFFICE

Mr. MALFI. Thank you.

Mr. Chairman and members of the committee, thank you for the opportunity to testify today about how homeland security is vulnerable to identity fraud.

Today, counterfeit identification is easily produced and used to create fraudulent identities. Tests we have performed over the past 3 years demonstrate that counterfeit identification documents can be used to enter the United States, purchase firearms, gain access to government buildings and other facilities, obtain genuine identification for both fictitious and stolen identities and obtain social security numbers for fictitious identities.

In conducting these tests we created fictitious identities and counterfeit identification documents such as driver's licenses, birth certificates and social security cards. We did this using inexpensive computer software and hardware that are readily available to any purchaser.

Our work shows how security vulnerabilities can be exploited. From July 2002 to May 2003 we counterfeited state driver's licenses and birth certificates with fictitious names and used them to enter the United States from the Western hemispheres, countries including Jamaica, Barbados, Mexico and Canada. Bureau of Immigration and Customs Enforcement staff never questioned the authenticity of the counterfeit documents and our investigators encountered no difficult entering the country using them.

Second, counterfeit drivers' licenses can be used to purchase firearms. Between October 2000 and February 2001 we used counterfeit driver's licenses with fictitious identifiers to purchase firearms from licensed dealers in five states: Virginia, West Virginia, Montana, New Mexico and Arizona.

When we purchased these firearms, the majority of the firearms dealers we dealt with complied with the laws governing such purchases, including instant background checks required by Federal law. However, an instant background check only discloses whether the prospective purchaser is a person whose possession of a firearm would be unlawful. Consequently, if the prospective purchaser is using a fictitious identity, as we did, an instant background check is not effective.

Third, counterfeit identification can be used to gain access to Federal buildings and other facilities. In March 2002 we breached the security of four Federal office buildings in the Atlanta area using counterfeit law enforcement credentials to obtain genuine building passes, which we then counterfeited.

We were also able to obtain building passes that authorized us to carry firearms in the building. As a result, several investigators, including one carrying a briefcase suitable for carrying firearms, bypassed the magnetometers and x-ray machines using the counterfeit building passes. Then they were able to move freely throughout the buildings during the day and evening hours. In April and May of 2000, we similarly gained access to numerous Federal buildings in Washington D.C. that contained the offices of cabinet secretaries or agency heads.

Finally, we easily obtained social security numbers for fictitious names. We used counterfeit identification documents to obtain valid social security numbers from the Social Security Administration for two fictitious infants. In addition, we visited two states and obtained authentic but fraudulent driver's licenses using the names, social security numbers and date of birth of individuals listed on the Social Security's publicly available master death file.

The master death file contains the names, social security numbers and dates of birth of deceased individuals. The motor vehicle departments in two of the states we visited are among those that rely solely on visual verification of identification documents and do not compare the information on licenses applications with the Social Security Agency's master death file.

Our work leads us to three basic conclusions. One: government officials and others generally did not recognize that documents we presented were counterfeit. Two: that many government officials were not alert to the possibility of identity fraud and some failed to follow security procedures. And three: identity verification procedures are inadequate.

While some of the problems revealed in our tests have been addressed by the responsible agencies, much remains to be done. The driver's license is the most commonly accepted document used for identification. The weaknesses we found during this investigation clearly shows that border inspectors, motor vehicle departments and firearm dealers need to have a means to verify the identity and authenticate the driver's licenses that are presented to them.

In addition, government officials who review identification need additional training in recognizing counterfeit documents. Further, those officials also need to be more vigilant when searching for identification fraud.

Thank you.

[The statement of Mr. Malfi follows:]

PREPARED STATEMENT OF MR. RONALD D. MALFI

Identification Documents Fraud and the Implications for Homeland Security

Mr. Chairman and Members of the Committee:

Thank you for the opportunity to testify today about how homeland security is vulnerable to identity fraud. Today, counterfeit identification is easily produced and used to create fraudulent identities. Tests we have performed over the past 3 years demonstrate that counterfeit identification documents can be used to

- enter the United States,
- purchase firearms,
- gain access to government buildings and other facilities,
- obtain genuine identification for both fictitious and stolen identities, and
- obtain social security numbers for fictitious identities.

In conducting these tests, we created fictitious identities and counterfeit identification documents, such as driver's licenses, birth certificates, and social security cards. We did this using inexpensive computer software and hardware that are readily available to any purchaser.

Our work shows how security vulnerabilities can be exploited. From July, 2002, through May, 2003, we counterfeited state driver's licenses and birth certificates, with fictitious names and used them to enter the United States from Western Hemisphere countries, including Jamaica, Barbados, Mexico, and Canada. Bureau of Immigration and Customs Enforcement staff never questioned the authenticity of the counterfeit documents, and our investigators encountered no difficulty entering the country using them.[1]

Second, counterfeit driver's licenses can be used to purchase firearms. Between October, 2000, and February, 2001, used counterfeit driver's licenses with fictitious identifiers to purchase firearms from license dealers in five states—Virginia, West Virginia, Montana, New Mexico, and Arizona. When we purchased the firearms, the majority of the firearms dealers we dealt with complied with laws governing such purchases, including instant background checks required by federal law.[2] However, an instant background check only discloses whether the prospective purchaser is a person whose possession of a firearm would be unlawful. Consequently, if the prospective purchaser is using a fictitious identity, as we did, an instant background check is not effective.[3]

Third, counterfeit identification can be used to gain access to federal buildings and other facilities. In March, 2002, we breached the security of four federal office buildings in the Atlanta area using counterfeit law enforcement credentials to obtain genuine building passes, which we then counterfeited. We were also able to obtain building passes that authorized us to carry firearms in the buildings. As a result, several investigators, including one carrying a briefcase suitable for carrying firearms, bypassed the magnetometers and x-ray machines using the counterfeited building passes. They then were able to move freely throughout the buildings during

[1] U.S. General Accounting Office, *Counterfeit Documents Used to Enter the United States from Certain Western Hemisphere Countries Not Detected,* GAO–03–713T (Washington, D.C.: May 13, 2003).

[2] 18 U.S.C. § 922(t).

[3] U.S. General Accounting Office, *Firearms: Purchased from Federal Firearm Licensees Using Bogus Identification,* GAO–01–427T (Washington, D.C.: March 19, 2001).

day and evening hours.[4] In April and May, 2000, we similarly gained access to numerous federal buildings in Washington, D.C., that contained the offices of cabinet secretaries or agency heads.[5]

Finally, we easily obtained Social Security Numbers (SSN) for fictitious names. We used counterfeit identification documents to obtain valid SSNs from the Social Security Administration (SSA) for two fictitious infants. In addition, we visited two states and obtained authentic but fraudulent driver's licenses using the names, SSNs, and dates of birth of individuals listed on SSA's publicly available Master Death file. The Master Death file contains the names, SSNs, and dates of birth of deceased individuals. The motor vehicle departments in two of the states we visited are among those that rely solely on visual verification of identification documents and do not compare the information on license applications with SSA's Master Death file.[6]

Our work leads us to three basic conclusions: (1) government officials and others generally did not recognize that the documents we presented were counterfeit; (2) many government officials were not alert to the possibility of identity fraud and some failed to follow security procedures and (3) identity verification procedures are inadequate. While some of the problems revealed in our tests have been addressed by the responsible agencies, much remains to be done. A driver's license is the most commonly accepted document used for identifications. The weaknesses we found during this investigation clearly show that border inspectors, motor vehicle departments, and firearms dealers need to have the means to verify the identity and authenticity of the driver's licenses that are presented to them. In addition, government officials who review identification need additional training in recognizing counterfeit documents. Further, these officials also need to be more vigilant when searching for identification fraud.

Mr. Chairman, this completes my statement. I would be happy to respond to any questions you or other members of the committee may have.

Chairman COX. Thank you, Mr. Malfi. And thank you for your leadership of the Office of Special Investigations.

That is hair curling testimony. We were sorry to receive it, but we intend to act upon it.

Our next, and final, witness is Keith M. Kiser, who is the chair of the American Association of Motor Vehicle Administrators, an organization of the departments of motor vehicles in all 50 states.

Mr. Kiser, welcome.

STATEMENT OF MR. KEITH KISER, CHAIR, AMERICAN ASSOCIATION OF MOTOR VEHICLE ADMINISTRATORS

Mr. KISER. Good afternoon, Mr. Chairman and members of the committee.

I am Keith Kiser, Chair of the Board of the American Association of Motor Vehicle Administrators, or AAMVA. AAMVA represents motor vehicle and law enforcement officials who are responsible for administering motor vehicle laws, driver credentialing and highway safety enforcement.

The state-issued driver's license is the most widely used and accepted form of I.D. in America. It is at the heart of our identification infrastructure and homeland security. Unfortunately, homeland security is threatened because licensing procedures are outdated.

Many states are taking piecemeal steps to improve the licensing process, and that includes California, despite passage of S.B.60. However, California's situation is not unique. Other states' policy

[4] U.S. General Accounting Office, *Security Breaches at Federal Buildings in Atlanta, Georgia,* GAO–02–668T (Washington, D.C.: Apr. 30, 2002).

[5] U.S. General Accounting Office, *Security: Breaches at Federal Agencies and Airports,* GAO/T–OSI–00–10 (Washington, D.C.: May 25, 2000).

[6] U.S. General Accounting Office, *Social Security Numbers: Ensuring the Integrity of the SSN,* GAO–03–941T (Washington, D.C.: July 10, 2003).

makers have weakened driver's license I.D. procedures by allowing undocumented aliens to obtain a license. This further compromises our nation's security.

A valid license opens doors and allows freedom of movement within society. It serves as identification to purchase firearms and to obtain benefits, credit, employment, and other federally-issued documents and potentially voting rights. Unfortunately, until we implement uniform practices to verify the validity of documents and the identity of the person holding them, the process will remain fragmented and vulnerable to fraud.

Recently, the AAMVA board passed two resolutions. One discourages the issuance of a photo driver's license to undocumented aliens. The other recommends it is premature to accept foreign consular cards for I.D. purposes.

"Why did the board take these actions?" Our mission is to serve those who are lawfully in this country. We have a responsibility and an obligation to preserve public safety and national security. As issuers of this document we must verify the identity of the license holder and ensure lawful residence to maintain reciprocity among the states.

Since October 2001, AAMVA has joined with numerous industry, advocacy and law enforcement experts to strengthen the licensing process.

As a result of this comprehensive approach, we recommend tightening application requirements; electronic verification of an applicant's driver's record and breeder documents; improved issuance procedures including internal audits and training for employees; increased penalties for those who commit fraud, and to ensure compliance with these activities participation by all states in the Driver's License Agreement, an interstate compact developed to address these issues.

Because DMVs do not have a real-time verification system, individuals apply for and obtain a license in more than one state. The findings of the recent GAO investigations are evidence of this weakness. To remedy this, we need an information system to ensure each driver has only one license, only one driver record, and only one identity.

In addition, the use of false breeder documents within the application process continues to grow. We must adopt a uniform list of acceptable I.D. documents relied on for license issuance; provide training to be a DMV employee so they can recognize and appropriately handle fraudulent documents; and ensure motor vehicle agencies have the ability to electronically verify the validity of breeder documents.

We also have a problem with fake licenses and I.D.s. They are easily altered or counterfeited. There are more than 240 valid license formats, all lacking uniform security features. To combat this problem, we need minimum uniform card design and security features for the license and then train other end-users to identify fraudulent documents.

The last problem we would like to address is people. We cannot legislate morality, but we can fight fraud on both sides of the DMV counter. AAMVA recently developed model internal controls of compliance procedures for states to adopt. In addition, Federal and

state policy makers must partner with law enforcement and the courts to implement and enforce stiffer penalties.

Over the last 2 years, AAMVA has discussed these problems with Congress and our Federal partners. The evidence is clear, it is time to implement the solution; a solution that is a comprehensive package and not a piecemeal fix; a solution that reduces identity theft and enhances homeland security; a solution that protects an individual's privacy by first verifying their identity.

In closing, two GAO investigations began with a different focus, but ended with the same recommendation: the Senate Finance Committee studied the facts and agreed with AAMVA that states need a driver's license information system to share driver records, exchange digital photos and verify birth and death records with vital statistics agencies.

The states cannot go it alone. The solution requires a state-Federal partnership that includes funding and political will. We need Congress's help.

Mr. Chairman, I thank you for the opportunity to be here. On behalf of all the AAMVA members we look forward to working with you.

[The statement of Mr. Kiser follows:]

PREPARED STATEMENT OF MR. KEITH M. KISER

Good Morning, Chairman and distinguished Members of the House Select Committee on Homeland Security. My name is Keith Kiser and I am the Director of the Motor Vehicle Division of the North Dakota Department of Transportation (NDDOT) and Chair of the Board of Directors for the American Association of Motor Vehicle Administrators (AAMVA). Thank you for the opportunity to testify on behalf of AAMVA to discuss the vulnerabilities in the driver's license application process and the document itself, its impact on national security and a comprehensive approach needed to fix the driver's licensing system.

AAMVA is a state-based, non-profit association representing motor vehicle agency administrators, senior law enforcement officials and industry in the United States and Canada. Our members are the recognized experts who administer the laws governing motor vehicle operation, driver credentialing, and highway safety enforcement. AAMVA plays an integral role in the development, deployment and monitoring of both the commercial driver's license (CDL) and motor carrier safety programs. The Association's members are responsible for administering these programs at the state and provincial levels.

We believe this hearing will generate critical public discourse about the urgent public policy issue of building more integrity into the driver licensing process.

BACKGROUND

AAMVA commends the House Select Committee on Homeland Security, for its focus on defining and showing the vulnerabilities with the driver's license and identification card. The state-issued driver's license is the most widely used and accepted form of ID in America. It's at the heart of our identification infrastructure and homeland security. Unfortunately, homeland security is threatened because of vulnerabilities in the driver's license system.

Why is this happening? Our current licensing structure and the credential that we issue were designed for another time and today's system is, at best, antiquated. The U.S. has more than 240 different, valid forms of passenger car driver's licenses and ID cards in circulation. Each state and D.C. has different practices for issuing licenses and reporting convictions. Individuals looking to undermine the system, whether a problem drinker, underage drinker, identity thief or terrorist shop around for licenses in those states with the weakest practices. Unfortunately, over-the-counter computer software and hardware is making it easier for individuals to produce counterfeit licenses and fraudulent breeder documents.

In addition, the lack of standard security features on a license allows individuals to exploit the system. This makes it difficult for law enforcement to verify the validity of a license from another state—not to mention the identity of the person holding it. This situation is worsened by the availability of counterfeit licenses and fraudulent breeder documents over the Internet and sold on the underground market.

Many states are taking steps to improve the licensing process. And, that includes California, despite passage of Senate Bill 60. However, California's situation is not unique. Other state policymakers have weakened driver's license ID procedures by allowing undocumented aliens to obtain a license through use of the IRS Individual Taxpayer Identification number, acceptance of foreign consular cards and non-secure "breeder" documents. This further compromises our nation's security. A valid license opens doors and allows freedom of movement within society. It serves as identification to purchase firearms and to obtain benefits, credit, employment, other federally issued documents, and potentially, voting rights.

Taking away the privilege to drive in this country is often viewed by both the federal and state legislative branches of government as an option to punish those who break the law. U.S. citizens can have their privilege to drive withdrawn for, among other reasons, poor driving behavior, failure to provide court-ordered child support—even failure to pay library fines. If DMVs are required to license undocumented aliens (who have by definition violated federal law) the illegals are in a sense receiving preferential treatment.

Also, such action places a state government agency as being essentially complicit in the violation of federal immigration laws. Once an undocumented alien obtains a driver's license, essentially that individual has no need for valid, federally issued immigration documents.

Recently, the AAMVA Board passed two resolutions.[1] One discourages the issuance of a photo driver license to undocumented aliens. The other recommends it is premature to accept foreign consular cards for ID purposes. Why did the Board take these positions? Our mission is to serve those who are lawfully in this country. We have a responsibility and an obligation to preserve public safety and national security. As issuers of this document, we must verify the identity of the license holder and ensure lawful presence to maintain license reciprocity among the states.

However, until we all share uniform practices to verify the validity of documents and the identity of the person holding them, the process will remain fragmented and vulnerable to fraud. As a result, we increase the opportunities for identity theft and put at risk our nation's national security and highway safety.

Shortly after September 11th, AAMVA members came together to develop a comprehensive solution to enhancing the licensing process. This comprehensive approach addresses:

- tightened application requirements for obtaining a driver's license,
- real-time verification of an applicant's driver history and breeder documents,[2]
- improved processes and procedures for issuance, including internal audit controls and training for employees, and
- increased penalties for those that commit credential fraud.

Vulnerabilities & Comprehensive Approach

The events of September 11th, caused a radical shift in the perception of risk and the use of a driver license or ID card. In October 2001, the AAMVA Executive Committee developed and passed a resolution establishing the Special Task Force on Identification Security. The Task Force concluded that there were a number of common issues needing to be addressed: administrative processing, verification/information exchange, the need for a unique identifier, the format of the driver's license/ID card, fraud prevention and detection, residency, and enforcement and control of standards. Based on the recommendations of the Task Force, AAMVA brought together knowledge, experience and expertise from across jurisdictional boundaries, federal agencies and stakeholder organizations to establish uniform identification practices and procedures to aid in the prevention of fraudulently issued driver licenses and identification cards.

The objective, with participation and recommendations from states and provinces, was to provide a guide to jurisdictions that would help standardize the process of identifying applicants in the 21st century. AAMVA divided the issues surrounding identification security into 14 subtopics, each subtopic being addressed by a task group.

AAMVA has identified and targeted the areas to fix what we believe are the problems with the current system. Let's look at the vulnerabilities in driver licensing. And more importantly, the steps needed to tighten the system.

First, individuals can apply for and obtain a license in more than one state, which the GAO investigators illustrated by using the same fictitious name and fraudulent documents in seven of the eight states. At this time, DMVs do not have an electronic method to verify whether a person has been issued a license in another state. We

[1] See Attachment 1 and 2.

[2] Breeder documents are defined as those documents used to confirm identity such as birth certificates, Social Security cards or immigration documents.

need to establish an information system that will ensure each driver has only one driver's license, only one driver record and only one identity. The findings of the GAO investigations are evidence of this weakness.

In the mid-1990s, AAMVA began exploring the possibility of having a system similar to the Commercial Drivers License Information System (CDLIS) for all drivers within the United States in order to better monitor the problem driver population. States need more effective tools to manage the driving records we already maintain. Problem drivers, who obtain multiple licenses, spread their bad driving history across the states. As a result, they avoid detection, penalties and punishment. By 1998, Congress recognized the potential benefits of such an information system and directed NHTSA and FMCSA to study the IT issues and costs associated with developing and operating this system. The report concluded an all-driver pointer system is feasible.[3]

We have witnessed the success of such a system through the use of CDLIS, which kept more than 871,000 potential dangerous truck drivers from obtaining a commercial driver's license between 1992 and 1996.[4] CDLIS is designed as a pointer system for commercial drivers. CDLIS limits commercial drivers to one and only one commercial driver's license and it has worked well for this purpose. Before CDLIS, it was possible for a commercial driver to apply for and obtain a commercial driver's license in a new state without acknowledging having an existing license in another state. This had serious implications for highway safety, since hiding the existence of another license could also hide a dangerous driving record. We need an all-driver pointer system that will direct one state where to find and accurately verify someone's driving histories in other states for all drivers, commercial and non-commercial. DMVs already exchange driver history on commercial vehicle drivers through CDLIS. An all-driver pointer system will help prevent identity theft and strengthen national security by limiting a driver to one license and one driving history.

Second, the use of false breeder documents to obtain an authenticate driver's license or identification card runs rampant within the application process. DMVs must adopt a uniform resource list for acceptable identification documents, which will narrow the numerous documents, relied on for issuing a license or identification card. After much research, AAMVA has recently concluded and issued the Acceptable Verifiable ID Resource List and Administrative Procedures.[5] By utilizing the lists, its procedures and future fraudulent document recognition training, motor vehicle employees should be able to verify that the applicant in front of them is who they are claiming to be and that documents presented are reliable. The use of the resource lists also promotes uniformity, identification reciprocity between jurisdictions, and helps protect the customer's personal information.

In addition, DMVs must provide adequate fraudulent document training to their employees. We need to give them the tools to recognize and appropriately handle fraudulent documents. The use of fraudulent documents has caused enormous economic losses in both the U.S. and Canada. The use of fraudulent documents to obtain driver's licenses/identification cards has grown exponentially in recent years. AAMVA in conjunction with the Federal Motor Carrier Safety Administration (FMCSA), the National Highway Traffic Safety Administration (NHTSA), the U.S. Secret Service (USSS), the Royal Canadian Mounted Police (RCMP) and the Canadian Council of Motor Transport Administrators (CCMTA) has developed a comprehensive model training program for Fraudulent Document Recognition (FDR).

The three-level FDR program is designed to assist states and provinces with the formal training of motor vehicle and law enforcement personnel in the recognition/detection of fraudulent identification documents. Level I address basic training needs for frontline employees and law enforcement officials. Level II addresses advanced training needs for motor vehicle supervisors, document examiners, law enforcement officials and fraud investigators. Level III addresses training at a forensic level and is slated for future development, if deemed necessary. Level I and Level II training materials were showcased during the 2003 AAMVA regional meetings. Formal Level I and Level II train-the-trainer sessions, designed to train jurisdictional fraud trainers, will be held between October 2003 and February 2004 in Rhode Island, Missouri and Utah. Based on available funding, future development

---

[3] National Highway Traffic Safety Administration in conjunction with Federal Motor Carrier and AAMVA, *"Report to Congress: Evaluation of Driver Licensing Information Program and Assessment of Technologies,"* 2001. (http://www.aamva.org/drivers/drv—AutomatedSystemsDRIVerS.asp#TechAssessment)

[4] Federal Highway Administration, Office of Motor Carrier Research & Standards Driver Division, *"Commercial Driver License Effectiveness Study,"* page 11, September 1998.

[5] American Association of Motor Vehicle Administrators, *Status Report to AAMVA Membership—Attachment 1 Acceptable Verifiable Resource Lists and Procedures,* July 2003,(http://www.aamva.org/Documents/idsAttach1StatReportJuly03.pdf).

may include training videos, educational brochures, self-study materials and computer-based and/or Web-based training. AAMVA will establish a maintenance program to update the materials on a regular basis. We invite members of the committee to attend any of the upcoming training sessions.

Furthermore, we must ensure motor vehicle agencies have the ability, preferably electronically, to verify the validity of source documents with issuing agencies, such as the Social Security Administration, Immigration and Naturalization Services, vital records agencies and other DMVs. Currently, 25 states are electronically verifying Social Security Numbers with the Social Security Administration. But that verification process needs improvement, which the GAO concluded in another report to Congres.[6] Too frequently SSA's automated system indicates that a number does not match, when in reality, after manual investigation, it is a match. This situation is deterring other states from using the SSA system. Congress must direct the Social Security Administration to improve their system so that this unnecessary, labor-intensive process can be eliminated. Each check of the system should also reference SSA's death records to ensure that a state does not issue a driver's license or identification card to an individual presenting personal information of a deceased person.

AAMVA is working cooperatively with the states and the Federal Motor Carrier Safety Administration (FMCSA) to pilot test three on-line verification systems:

• Online Verification of Driver Licenses—this allows states and third parties, such as airports and banks, to electronically query and verify that a license presented to them was actually issued by the state shown on the face of the license. Once rolled out nationwide, this effort will greatly inhibit a criminal's ability to use counterfeit driver licenses.

• Interstate Digital Image Exchange—this allows states to exchange digital driver photos so that they can compare the picture to the individual standing in front of the clerk applying for a license. Once rolled-out nationwide, this will inhibit imposters from obtaining licenses and ID cards under another person's identity.

• Online Verification of Birth Certificates—this allows the states to electronically interact with the National Association for Public Health Statistics and Information Systems (NAPHSIS) to check state vital statistics records to determine the validity of a birth certificate being used to establish identity as part of the driver licensing program. Once rolled-out nationwide, this will inhibit the criminal's ability to use counterfeit birth certificates to obtain a driver license or ID card.

These are very worthy efforts and, on behalf of the states, AAMVA thanks Congress and FMCSA for providing the seed money to get them going. But they are not fully effective unless all of the data is available and all of the states are participating. The states need the help and support of Congress to get these programs rolled-out nationwide.

Third, the driver's license document is easily counterfeited. The current variety of documents and lack of uniform security features makes it easy for criminals to alter a real document or create a counterfeit. We must provide fraudulent document training to not only DMV employees but stakeholders to thwart acceptance of fake documents. The GAO investigators showed how easy it was to create and alter a driver's license and breeder documents using inexpensive commercially available software and hardware. Also, motor vehicle agencies must establish better procedures for removing fraudulent documents when an employee realizes the documents are fraudulent. We cannot afford to give the fraudulent documents back to the perpetrator and law enforcement needs to be notified without endangering the DMV employee. However in some instances, DMV employees inform individuals that produce fraudulent documents to obtain a driver's license or ID card the correct procedure to apply for a document. There is a delicate balance between customer service, safety and security.

Additionally, motor vehicle agencies need to adopt minimum, uniform card design and security specifications for the driver license document. To secure jurisdiction-issued driver's license/ID card credentials, the association examined card functionality, visible data and card layout, machine-readable data elements, machine-readable technology (MRT), document security features, and other card design elements and considerations. AAMVA, working with a wide variety of stakeholders, has developed those minimum specifications and they are now available for use by the states.

The fourth problem relates to people. For some, this comes with the vulnerability to criminal behavior, which can result in stolen DMV equipment and inventory and the acceptance of bribes. Individuals are breaking into DMV's, stealing equipment

[6] General Accounting Office, *Improved SSN Verification and Exchange of States' Driver Records Would Enhance Identity Verification,* GAO–03–920, September 2003.

and inventory to produce documents. AAMVA is developing model procedures for security and inventory controls. DMVs and all identity issuing agencies need an information system to post alerts when equipment or inventory is stolen. Currently, through AAMVA's Web site, the association posts alerts regarding official federal, international or state documents and equipment that is stolen.

We must provide online verification of the driver license and ID card. This will render stolen equipment and inventory useless. Any driver licenses or ID cards created on stolen equipment would be rejected in the verification process because the state's database would not contain information pertaining to those cards.

Unfortunately, individuals bribe DMV clerks to issue driver's license or ID cards. It is a lucrative business. We cannot legislate moral behavior, but we can fight fraud on both sides of the counter. However, we need to implement stronger internal controls and auditing procedures that detect this behavior and prevent it from spreading. And, we must implement stiffer penalties and enforcement for those who choose to break the law.

Fifth, we must protect an individual's privacy while trying to bring the driver's license system into the 21st century. DMVs adhere to some of the strongest privacy laws on the books—the Driver's Privacy Protection Act. DPPA prohibits DMVs from selling your driver record information for commercial purposes without your prior consent. We'd like to make them stronger. The AAMVA Board of Directors passed a resolution stating that the association does not support the practice of collecting people's personal information from a driver's license for the purposes of marketing or building customer databases—without the full knowledge and consent of the license holder. We advocate that people or organizations scan the driver's license only to verify and not to capture information. Furthermore, in May 2003, the AAMVA Board endorsed eight privacy principles based on the Global Privacy Design Principles.[7] The principles address openness, individual participation, collection limitation, data quality, use, disclosure limitation, security, and accountability. Therefore, AAMVA is assessing the impact of DL/ID security improvement on personal privacy and will develop best practices and model guidelines for motor vehicle agencies to inform citizens of personal information protection.

CONCLUSION

These problems exist and are interstate in nature. The only way to ensure that the proper fixes have been applied is for all states to follow the same roadmap. Inconsistent remedies from state to state will leave open the loopholes that exist today. The solution:

- must be implemented as a package and not as a piecemeal fix.
- will reduce identity theft and enhance homeland security and highway safety.
- can be accomplished without sacrificing an individual's privacy by verifying their identity.
- can only be achieved with a federal-state partnership. Without a federal-state partnership to implement the solutions, this comprehensive approach is little more than a best practice.

First hand you have witnessed the vulnerabilities of the current process. Two GAO investigations began with a different focus but ended with the same recommendation. The Senate Finance Committee studied the facts and agreed with AAMVA that states need a driver's license information system to share driver records, exchange digital photos, and verify birth and death records with vital statistics agencies.

AAMVA seeks funding for the Birth and Death Records Verification Program, and Digital Image Exchange program discussed in my testimony, to improve the states drivers licensing system. We are grateful that the Treasury-Transportation appropriations subcommittee included critical Report language in the FY04 transportation appropriations bill related to the funding of these programs. We commend Chairman Istook for recognizing their importance and his willingness to take action. However, we are hoping that the language can be strengthened in Conference to ensure these pilot programs stay on track. There is a real concern that if the funding is not provided, fraudulent driver's licenses and ID's will continue to be issued to potentially dangerous individuals.

Additionally, we seek funding in the TEA—21 reauthorization bill to improve the Commercial Drivers license information system and to build toward a nationwide all drivers license information system. We would ask for your help in securing this authority and funding in the highway bill.The states cannot go it alone. The solution

[7] American Association of Motor Vehicle Administrators, *Status Report to AAMVA Membership—Attachment 4 Privacy Principles,* July 2003, (http://www.aamva.org/Documents/idsAttach4StatReportJuly03.pdf)American Association of Motor Vehicle Administrators

requires a state-federal partnership that includes funding and political will. We need Congress' help.

Thank you. I've concluded my testimony and welcome any questions from the subcommittee.

AMERICAN ASSOCIATION OF MOTOR VEHICLE ADMINISTRATORS (AAMVA) BOARD OF DIRECTORS RESOLUTION 03–08 USE OF FOREIGN CONSULAR CARDS FOR IDENTIFICATION PURPOSES

WHEREAS, the Association has developed an Acceptable Verifiable ID Resources List that includes documents issued by the U.S. and Canadian agencies and organizations that are recommended for use by DMV employees to verify that a person applying for a driver's license or ID card is who he/she is purporting to be; and

WHEREAS, the verifiability of the documents by the issuing agencies was an important factor in considering documents for inclusion on the Acceptable Verifiable ID Resources List: and

WHEREAS, many member jurisdictions have expressed concerns that foreign consular IDs, including Mexico's matricula consular card, lack standardized issuance procedures, uniform security features, and a secure database for verification purposes; and

WHEREAS, the AAMVA Board of Directors recommends the continued use of the foreign passport as an official identification document, and

WHEREAS, AAMVA is in the process of gathering information on other foreign consular ID documents and their possible use for identification purposes; and

THEREFORE BE IT RESOLVE, that the AAMVA Board of Directors believes that it is premature to recommend the use of any foreign consular ID, including Mexico's matricular consular card, at this time, as more information is needed to assess the verifiability of these documents.

BE IT FURTHER RESOLVED, that legal and diplomatic issues also warrant further review and consultation with the United States Department of State as they relate to possible conflicts with the Vienna Convention on Consular Relations and Optional Protocols of 1963.

RESOLVED FURTHER, that the AAMVA Board of Directors accepts and endorses as an AAMVA standard that no other foreign documents be allowed to provide specific data for identification purposes other than foreign passports. A foreign passport in conjunction with the proper immigration documents (i.e. I–95 for the U.S. is necessary if used to validate legal presence.

Board of Directors Resolution No. 03–O8 was passed at a meeting duly held on May 17, 2003.

Betty L. Serian
Chair of the Board

Stacev K Stanton
Chair of the Board

AMERICAN ASSOCIATION OF MOTOR VEHICLE ADMINISTRATORS (AAMVA) BOARD OF DIRECTORS RESOLUTION 03–08 POSITION ON ISSUING DRIVER'S LICENSES TO UNDOCUMENTED ALIENS

WHEREAS, in order to strengthen the security of the photo driver's license and the issuance process associated with it, it will be necessary to tighten the standards proving one's identity in order to obtain a license; and

WHEREAS, the Board of Directors approved a minimum list of Acceptable Verifiable Identification Resources for verifying an applicant's residence, identity and legal presence; and the documents included are required to be original or certified copies from the issuing agency.

THEREFORE RE IT RESOLVED, that raising the bar of proof regarding the validity of source documents for everyone strengthens uniformity and encourages reciprocity in motor vehicle administration and enhances highway safety enforcement; and

BE IT RESOLVED FURTHER that it is the recommendation of the Board of Directors of the American Association of Vehicle Administrators that jurisdictions not grant a photo driver's license or photo ID card to undocumented aliens.

Board of Directors Resolution No. 03–09 was passed at a meeting duly held on September 4–5, 2003.

Betty L Serian
Chair of the Board

Chairman COX. I thank each of the witnesses for your outstanding testimony.

the bells that you heard ring are a recess on the floor, subject to call the chair, so we expect that we will not have a floor votes for another hour or so. And that is good news; these hearings are often interrupted by work on the floor, and that will not happen to us just yet.

I would like to recognize myself for 5 minutes of questions. And begin where we just ended up, Mr. Kiser, with you.

You are recommending that the Federal Government take action in an area that has traditionally been one of state jurisdiction. I think most members of Congress want to be very, very careful about the federalism implications here.

We do not want to do what is not Congress's business, we don't want to take over state DMVs, we don't want to tell them exactly how and what they may do. On the other hand, we have a national system, in which, for example, in the Western hemisphere, any U.S. citizen can cross our border going out or coming in merely by showing a driver's license, which is supposed to be prima facie evidence of—not just prima facie, but satisfactory evidence of citizenship, or at least the right to be legally in the country. So we have a lot riding on this.

We have also got, by the GAO's estimate—correct me, Mr. Malfi if I am wrong—about 240 different variations of driver's licenses and I.D. cards issued by jurisdictions within the United States, so that for border guards this is a very difficult job.

Likewise, we heard about the gun shows and gun dealers; we heard about entrance to Federal buildings; we heard about all manner of uses of these driver's licenses, and in each case the security workers, the Federal or state employees of the civilians, whose job it is to assess the validity of this I.D. are relying on an imperfect computer between their ears that supposed to keep straight these 240 different forms of identity.

Aren't we just riding for a fall here?

Aren't we in great need of using technology to help sort this out? And isn't standardization, uniformity and objectivity the aim, so that, for example, biometric identification will be part of matching the person to the I.D.

And I am going to address this question to you, but let any member of the panel join in.

Mr. KISER. Thank you, Mr. Chairman.

In my testimony I mentioned that we need a state and Federal partnership. It is clear to me in talking to my counterparts in the administration of driver's license laws that there is a clear recognition that there is a problem. And the problem is growing and is massive.

It is also clear that it is in the administrative area that we don't have the authority to really fix that, that is a legislative decision.

Chairman COX. When you say that you don't have the authority, you mean AAMVA?

Mr. KISER. We mean AAMVA, but also as a jurisdictional member, it takes legislation in my jurisdiction and in each jurisdiction

to create the changes, such as those described in Virginia. So it takes a political will to do that. And it also takes—

Chairman COX. Let me just interject.

When the Federal Government very explicitly says, "Don't use the taxpayer identification number for any identification purpose outside the tax system, because it is not reliable," and when a state then passes a law that does exactly that, what should be the response of the Federal Government, assuming we want to be sensitive on the federalism point?

Mr. KISER. Mr. Chairman, I wouldn't try to speak to what the response of federal government.

Chairman COX. But given the existing partnership between the states, who are your members, and the Federal Government, we want to be sensitive to the separate allocation responsibilities. What happens when a state so miserably fails?

Mr. KISER. I think, Mr. Chairman, if that state miserably fails it may be appropriate for the Federal Government to take some level of action. What that is, I am not sure.

I do think that it is important that we recognize—as I believe someone said earlier—that different jurisdictions, different states have different levels of response to their own situations. Again, AAMVA's position is that you should not honor those documents that don't have security. We are not a regulatory agency, we don't have the ability to impose our will or the will of The AAMVA organization, onto a particular jurisdiction.

Chairman COX. Mr. Carico, you mentioned that the law changed in Virginia, requiring people to show proof that they were who they said they were, that they were legitimately in the country so that the 9/11 hijacker scheme couldn't be repeated.

In California, we have changed our law to go in the opposite direction, so you explicitly do not have to provide such information. What do you believe the Federal Government should do? You represent a state; can the Federal Government be aggressive in this area, do we have to be supine, or are we just going to let it happen? What can be done?

Mr. CARICO. I think the main thing the Federal Government can do is help in the information sharing process between the states. In Virginia, we also have the Federalist concerns that you do, but the Federal Government has a bigger repository for a lot of different kinds of information. And I know in the criminal area, like that National Crime Information Center, the NCIC, has a lot of information that is available to the states. If someone comes up on criminal charges or something in the states—I was a former prosecutor—we often used that vehicle of information in order to more effectively go after criminals.

The same can be done by the Federal Government. But I think we have to be careful, like Mr. Cox was saying, we need a Federal-state partnership, not only in the information sharing arena, but the Federal Government can encourage these states in the dangers of using the tax identification numbers. The Federal Government has a responsibility to educate the states as to the dangers of using these numbers. These numbers are rotten.

Chairman COX. And do you think the Federal Government has failed in its responsibility? I mean who in the world could not know

this, it is posted on the website; I mean there is no question about this.

Mr. CARICO. I don't think that the Federal Government has failed, I think the states have failed to listen and failed to heed the dictates from the Federal Government when it comes to saying, "Hey, we don't think you should use these numbers, you need to use more reliable numbers." And the states who are going in the opposite way have failed to learn the lessons of 9/11.

Chairman COX. And therefore?

Mr. CARICO. And therefore—again I think the Federal Government just needs to help educate and reiterate to the states and help to facilitate information sharing between the states when it comes to these types of issues.

Chairman COX. Well my time has expired. I think we are beginning a discussion on this and other members can carry it forward.

In order of appearance, Ms. Holmes Norton is next.

Mr. DEFAZIO. Excuse me, Mr. Chairman. I was here before any other member was in the room and sat here. So how could that be?

There was no other member in the room. I asked if the hearing was really at one o'clock because there was no one else here.

Chairman COX. I am sorry, we were just using the list that was provided by the minority for order of recognition of members.

Mr. DEFAZIO. Nope, they are shaking their head.

Chairman COX. I am happy to recognize the gentleman if there is no objection.

Mr. DEFAZIO. Well, I know I was here and there was no other member here, Mr. Chairman. The minority is shaking its head. I am just curious.

Ms. NORTON. Rather than have this deducted from the gentleman's time, I would be very pleased to defer to the gentleman.

Chairman COX. OK.

Mr. DEFAZIO. Thanks.

Chairman COX. The time belongs to the gentleman from Oregon, Mr. DeFazio is recognized.

Mr. DEFAZIO. Thank you, Mr. Chairman. Not on my time, but I have raised this issue previously with the minority side and they are now—it is just if you want members to come and be here on time, it is helpful.

Mr.—is it Pistole, Pistole, how do you pronounce it?

Mr. PISTOLE. It is Pistole, the "e" is silent, sir.

Mr. DEFAZIO. OK. All right. OK. So when I pronounce it, it will be right anyway.

Mr. PISTOLE. Thank you.

Mr. DEFAZIO. You raised an interesting point: who people purport they are. If I give you—if I apply, you are a private sector, I come to you, I apply for a job. I give you my name, I give you my social security number, you say, "I am going to run a background check." You put it into NCIC or a credit report, what do you get out of that?

Mr. PISTOLE. You get whatever records are in there, obviously, but it depends on the legitimacy and the validity of those underlying documents.

Mr. DEFAZIO. Or, whether that person has—how do you know I am that person?

Mr. PISTOLE. Exactly. So even though the name may be legitimate, how do we match it up with the person who has presented it to them? That is the underlying issue from our perspective.

Mr. DEFAZIO. OK. So then to Mr. Verdery, do you fly commercially as a passenger?

Mr. VERDERY. Yes I do.

Mr. DEFAZIO. OK, I see. Because your portfolio is the Transportation Security Policy, OK?

Mr. VERDERY. Yes, sir.

Mr. DEFAZIO. Do you go through the security?

Mr. VERDERY. Yes.

Mr. DEFAZIO. OK, so you go through the screening?

Mr. VERDERY. Yes.

Mr. DEFAZIO. OK. Do you think that it is necessary that we should be putting people through that screening at airports?

Mr. VERDERY. Of course.

Mr. DEFAZIO. OK.

Now do you think we should be putting people through that screening regardless of whether we know who they are or not? For instance, if I—if you don't know who I am, I should go through the screening even if we knew you were that person you should go through the screening. That is correct?

Mr. VERDERY. Well, yes. Of course the point of the screening, primarily, is to make sure that the person who is going to be getting on the plane is not a threat to the plane itself.

Mr. DEFAZIO. OK. Or on the plane, or is the idea of keeping those materials out of the airplane terminal where passengers, once they have gone through screening could accept something from someone else.

Mr. VERDERY. Right. And that is why the screening checkpoints are set up before the gates.

Mr. DEFAZIO. That is correct. OK.

Now we just heard from Mr. Pistole that if I give someone my social security number and a name, or a social security and a name, that is a meaningless background check. Would you agree with that, since we don't know whether that is really—we didn't check fingerprints, we didn't go to that point.

Mr. VERDERY. "Garbage in, garbage out."

Mr. DEFAZIO. OK. Are you aware that currently TSA exempts, at many airports has made it optional, that employees of vendors, that is people who work at McDonald's, Borders, once they have undergone a so-called "background check" that is, they gave their name and their social security to McDonald's or Borders is allowed to enter the terminal freely without going through security?

Are you aware of that policy?

Mr. VERDERY. Yes.

Mr. DEFAZIO. Well, how does that make sense with what you just told me? We know you are from the TSA, you know I am a member of Congress, I have got to have everything searched.

We don't know who this person is; we know they work at McDonald's. We don't know if they are the person who said they are at McDonald's, he has already told us, you said, "Garbage in, garbage out." He told us there is a real problem here, but we are allowing

those people wearing coats, carrying things, to go freely in—how secure is this system?

Now, what I have heard from TSA before is, "Well they are not getting on planes, congressman." A: they might have an e-ticket in their pocket, so we don't know that. B: they could be bringing something in to another person who went through security, who is a problem, who is getting on a plane.

Now how can you justify that? Isn't this a little bit of a loophole?

Mr. VERDERY. Well it is clearly a weakness in the system. As you know, TSA, working with DHS, is working on a broader initiative, the TWIC, the Transportation Worker Identification Card.

Mr. DEFAZIO. But today, several hundred thousand people, who we don't know, we don't know if they are the person they said they are, will file into secure areas of airports in the United States of America without even walking through the magnetometer, which of course wouldn't find explosives or—doesn't find a whole lot of other things—without putting what they are carrying on a belt. They just walk through.

They flash their McDonald's worker I.D. card at someone and they walk in. And you are saying this is a little bit of a problem. Don't you think this is a huge problem? Isn't the whole thing a lie for the traveling public? We are harassing the pilots, we are the harassing the flight attendants, we are checking every other passenger, we are checking you, working for TSA, head of transportation policy, we are checking members of Congress.

But the McDonald's employee, who may or may not have given a fake name and I.D. is allowed to carry whatever they want in or out of the airport and we are not concerned and we are not going to do anything about it. Or if we might get them a TWIC someday; how long has it been that this has been going on?

Mr. VERDERY. Well the TWIC has been underway for several months.

Mr. DEFAZIO. Right. But I mean how long have these people been going in and out of the airport without going through security?

Mr. VERDERY. I am not aware of the duration of that regulation.

Mr. DEFAZIO. Well why does that regulation exist? Why would we not want the McDonald's employees to go through the same security as the airline pilot when going to a secure part of the airport where they could be carrying contraband that could be used to take over a plane or blow up a plane? Why don't we want them to go through the same screening as an airline pilot?

Mr. VERDERY. Well, as you mentioned, they are going through a background check.

Mr. DEFAZIO. The background check, as you just admitted, "Garbage in, garbage out" and Mr. Pistole told us it was meaningless. All they do is give a name and a social security number.

Mr. VERDERY. If the assumption is that the data that is being provided in inaccurate.

Mr. DEFAZIO. Well the assumption—do you think McDonald's is taking fingerprints and checking these people, really doing a real background check on these people?

If they don't have a real background check, why don't they go through security?

The pilots, we know who they are, they have been fingerprinted. We know who they are, don't we? We really know they are that person with that I.D., that is actually a pilot for United Airlines, who has been doing this for 25 years. Everything on him and everything in his carry-on has to go through security. There is a McDonald's worker, we don't know who they are, we haven't fingerprinted them, we don't have the slightest idea of their identity, "Hey welcome to the airport!"

Now what sense does this system make? I have been trying to get TSA to pay attention—"Oh, we are working on a TWIC, congressman." Today four hundred thousand people will file in and out of the airport, we don't know who the heck they are or what they are carrying, but we are working on a bureaucratic solution here.

Mr. VERDERY. If I am wrong, and I would be happy to get back to you, my assumption is that the background checks are not being performed by McDonald's or by Borders, they are performed by the airport.

Mr. DEFAZIO. They are performed by commercial vendors who—what do they check? Do you know what they check?

Mr. VERDERY. I don't know.

Mr. DEFAZIO. They check the name and the social security number which Mr. Pistole and you just admitted is worthless if we don't know that is really the person with that name and that social security number, isn't it?

Mr. VERDERY. I mean the broader issue is that we don't have confidence in the document, say a driver's license because we are not sure.

Mr. DEFAZIO. But the broader point is, we don't even have to have, we don't even need a counterfeit document. You go to the death list, you get a legitimate name of a person and a legitimate social security number and you would adopt that, with approximately the same age as you.

We are never going to, McDonald's is not going to get to, the airport isn't going to get to whether or not that is really that person. So shouldn't that person go through security? Shouldn't all these four or five hundred thousand a day go through security, just like the pilots and the flight attendants and the frequent fliers and the TSA guy and the members of Congress? Isn't this an incredible loophole? Don't just tell me, "Oh, it is a little problem." It is a big problem. We don't know who they are.

I am not even talking about the other side of the airport, which is everybody who has access to the planes, of course we did find a few box cutters in the seats on planes after 9/11 probably put in there by cleaners. We are doing the same background check on cleaners, which is, "We got your name and social security number. We will run it through the system, if it comes back clean, if you didn't happen to steal the name and social security number or misappropriate it of a felon, you are fine."

Chairman COX. The gentleman's time has expired.

But you are certainly eligible to answer the question.

Mr. VERDERY. Obviously congressman, it sounds like you have had interaction with TSA on this directly, I am not privy to that, but I would be more than happy to go back and work with them

on this. It is not an issue I have worked with them directly on in my few months on the job.

But just more broadly, if I could just take a second, if we don't have confidence in a driver's license or another document because there are no security features, there is no check on what it takes to get a document, then we go back and revise what the driver's license is used for. Basically, if there is no security then we have to assume that a driver's license only proves that you went and took a driving test and maybe that you proved that you have car insurance, but nothing else. And that would implicate quite a bit, whether it is Federal buildings, getting on a plane, gun shows, whatever. I mean the whole reliance on driver's license—the example you raised a fairly legitimate one—but it is one of many that is caused by the weakness in the driver's license system.

Chairman COX. Thank you, gentlemen.

And I would note, that in some senses these are solvable problems and that today's hearing is focused on the ability, for example, of a known terrorist who acquired, not just a fake I.D., but one issued by the government that has the perfect imprimatur of legitimacy. And then to use it to freely gain access to places that he or she ought not to be.

The separate question of people who undergo background checks and who work within secure perimeters are beating our chests, is certainly one worthy of consideration by this committee and I think we ought to pursue it.

Next in order of questions, we will go to the gentleman from Michigan, Mr. Camp is recognized for 8 minutes.

Mr. CAMP. Thank you, Mr. Chairman. Mr. Verdery, you in your written testimony talk at some length about the driver's license and that 21 states don't require any proof of legal status. And it seems to me that that is an area we have a real concern, and particularly with the recent California law allowing people that are known non-citizens to acquire driver's licenses, which then has access to many other identifying documents.

Do you have any recommendations about changing what should occur in those sorts of identifying documents?

Mr. VERDERY. There are a couple things I would say in response to your question.

The administration is looking carefully at a whole range of document issues. I testified a few months ago at another committee at this body regarding the matricular consular, which is an issue which I would maybe raise today. In light of that issue and others, we are looking carefully at how the Federal Government should be encouraging states and others to come up with more secure documents. One area I would like to mention though, which hasn't come up particularly in the Q and A, or in the testimonies, is the positive things that are going on in terms of foreign documents.

In terms of foreign governments with their passports, in terms of the United States government issuing visas, in terms of the United States government issuing passports to U.S. citizens, those are all going to be biometrically enhanced over the next couple of years as a result of legislation that Congress passed and that we are implementing.

And so a lot of the problems, in terms of foreign documents, are going to be addressed; we will be able to lock in people's identities as biometrics, whether foreigners come in this country or a U.S. citizen.

So there is positive news here. Clearly on the driver's license front there is a lot of work to be done and I think one thing that should be considered is, rather than trying to come up with a one-size-fits-all, we ought to have one feature of a card that is secure that could be worked across all the various states that is secure and gives us some ability to believe that the person is who they say they are.

Mr. CAMP. Well, my concern too, is in your written testimony, also outlined at some length, how you get into this country from Canada or Mexico, and it is simply a verbal declaration that you are a resident is sufficient under the rules to allow admission.

Mr. VERDERY. That is correct.

Mr. CAMP. Do you have any recommendation in terms of changing that or making that more secure. Because it would seem to me that, yes, I understand in your testimony that the agent at the border will have an opportunity to go deeper and ask for written documents, but for the most part, that doesn't happen.

What should be done there? You lay out the current situation, but I wonder what you think we ought to do to tighten it up, to make sure that we don't have terrorists that come into this country by simply declaring they are citizens and being allowed to pass through.

Mr. VERDERY. We are looking very carefully at both the requirements, or relative lack of requirements on U.S. citizens that are returning to the country and also the Canadians and others who are coming into the country. As you know, any types of change, in terms of the Canadians, would raise some serious foreign policy considerations that need to be factored in.

We are working on that as part of the U.S.-VISIT System, which was mentioned previously. There will be tracking at land borders down the road, we have to work with the Canadians and the Mexicans who are coming in across the country to try to figure out how they fit into U.S. VISIT. So there is work being done. The current situation of an oral declaration is clearly a problem, notwithstanding the good efforts of our CBP inspectors in trying to enforce it.

Mr. CAMP. Obviously, we have a lot of back and forth across the border and we obviously want to facilitate legitimate travel, but I wondered what direction you see these discussions taking. I appreciate you are working on it, but I wondered where do you see this going or can you report to this committee the direction that you see these sorts of discussions going.

Mr. VERDERY. Well as we implement the VISIT System, I think we are headed towards a situation of tighter documentary requirements. I can't sit here today and promise you exactly what that is going to be, that is going to be decided by negotiations with our foreign partners, by an interagency process that is not yet complete.

We are headed in a direction where there will be more security, but we are not there today.

Mr. CAMP. OK. Thank you.

Mr. Pistole, you touched on some of the reasons and consequences of identity theft and fraud and I know of, in June, Steve McGrath from the FBI testified before the Judiciary Committee about the consular I.D. cards and the security implications. And I wondered if you could update the committee. Anything the FBI is doing to inform other agencies and state and local governments about those security implications and just sort of, what the status is of that particular issue.

Mr. PISTOLE. U.S. Congressman the FBI is working through the interagency process to assess the vulnerabilities that are associated with those particular cards, based on the lack of verifiable underlying data for the recipient to obtain the card. We are working with state and of course, the DHS, to try to identify those cards that are out there now that may pose a risk from previously issued, and then trying to move forward on a perspective move to see if there is a consensus to change that policy.

Mr. CAMP. Is there a Federal working group or task force on this issue?

Mr. PISTOLE. Yes.

Mr. CAMP. And is the FBI involved in that?

Mr. PISTOLE. Yes, with the Department of Justice.

Mr. CAMP. And tell me how that is going.

Mr. PISTOLE. We are making progress in general terms, but again, there is a government-wide decision that has been made that we dealing with from a threat-assessment perspective, and the FBI is one small part of that as representative to DOJ.

Mr. CAMP. OK. Thank you very much.

Thank you, Mr. Chairman.

Chairman COX. Thank you, gentlemen.

The gentle lady from Washington, Ms. Holmes Norton.

Ms. NORTON. Thank you very much, Mr. Chairman.

I am interested in prosecutions and enhanced penalties. I compliment Mr. Howard for the 50 arrests, the prosecutions we have had here. I recognize they are given with documents to look like in your and other offices across the country. The model from the country is often used, of course we know that if you are talking about undocumented immigrants, they don't have a lot to lose. They go across and they come right back. They of course, are not the people I am most interested in. I am interested in potential terrorists.

I sent for the statute you testified to, Mr. Howard, and I in certain parts of that statute I fully endorse the Identity Theft Penalty and Enhancement Act, but to refresh my recollection, I sent for a summary and I don't—either we need a new statute in order to deal with the problem we are talking about in this hearing, or we would seriously need to rework it.

The first problem I noted was that it deals with means—it really is an identity theft statute and it deals with identification using a means of identification of another person; whereas in the matter before the committee, we are dealing with probably fictitious persons altogether.

Now they call for 5 years imprisonment for specified felony violations, I have got a question for you. First of all, what is the jail penalty, the prison penalty today that you are working with and

under what statute? Is all identity activity a felony, or is some of it considered to be misdemeanor activity? I ask you these questions on the matter of fact that I think this committee may need to work on an entirely separate statute, now pending before Judiciary, may not even be able to be fixed to meet our concerns.

Yes, sir.

Mr. HOWARD. The statute we are working with now has 20 year penalties. The proposed statute has penalty enhancements of up to five years.

Ms. NORTON. You are working with a statute that has 20 years felonies?

Mr. HOWARD. Twenty year felonies.

Ms. NORTON. What is it?

Mr. HOWARD. That would be either 18 USC 1546, which is "Use of false I.D. documents."

Ms. NORTON. But these are all felonies?

Mr. HOWARD. Everything we are talking about is a felony. And the proposed statute has a five year enhancement. As I said, we would be glad to work with Congress. Certainly one of the things we see is might be more of a sentencing commission concern, in that some of the statutes have base levels that only provide penalties of 24 months, 2 years.

Ms. NORTON. What is the maximum we have been able to get here in the District of Columbia.

Mr. HOWARD. So far, Mr. Gonzalez–Gonzalez's 52 months, which is about four and a half years, but that was not based on the statute itself, he had prior convictions, which allowed us under the sentencing guidelines to move that penalty up to the total of 52 months.

Ms. NORTON. Would you like to see enhancement—I mean you would rather have 20 years, but I am trying to figure out.

Mr. HOWARD. I think the government would. Clearly one of the issues that we have when we are looking at these cases are individuals who come in and there is other information we want from them. For instance, if they are, as Mr. Gonzalez–Gonzalez was doing, importing documents from other states, we want to know who that person is.

Clearly, if they are willing to do the jail time, they are willing to take the penalty we have no leverage, in terms of trying to get them to cooperate with us.

Ms. NORTON. I would like very much to look into that.

I have a final question for all of you. It as a very controversial question, a very controversial issue. The chair spoke about 240 different kinds of I.D. and I frankly think, thinking about what you do. We are asking you to do something close to the impossible, and you are trying to somehow conform all of this. And ultimately it can all become circular as you probe deeper and deeper to find the ultimate document, the ultimate identification.

And I think part of the problem is we are dealing with retail remedies, after all it was undocumented immigrants looking for work before. If you are dealing with terrorists, it seems to me, we have got to get beyond the retail. And we have got to get beyond the state-by-state.

Now I am a card-carrying civil libertarian, I practice civil liberties in the courts, and kind of had a gut reaction against the national I.D. card. There are many people like me, libertarians and civil libertarians, who have begun to rethink that matter, because there are much more intrusive actions that the government is using in order to discern identity and because—I will give you an example, ultimately what we are using is racial profiling finally, when we can't think of anything else to do.

I don't know if the national I.D. card would finally get to the root of the problem or not. You can counterfeit those although probably less easily than counterfeiting all of these birth certificates and 240 other documents.

I am really looking for something beyond the retail that produces less intrusion into the privacy of the American people and greater security. So I am forced to ask the question about a national I.D. card and ask whether you think that would in fact, eliminate some of these problems or whether we would still have a problem even with a national I.D. card?

Chairman COX. The gentle lady's time has expired. But you have put such a predicament on the table here that I am sure we can allow at least 20 minutes for response.

Mr. HOWARD. I would be glad to give you two. It is certainly a—I think you hit it on the head congresswoman—it is a huge problem.

And it is one that the Justice Department is certainly studying and trying to get a hold of. Certainly as I go through a lot of our cases, the people that we are finding are simply opportunists and they are working with people, getting money from folks who are looking for opportunities in this country. I think the whole Justice Department, and certainly my office, and I know Mr. McNulty's office is very cognizant of issues of racial profiling and we want people who belong here, who are here legally and who are residents to enjoy that freedom. By the same token, we try to get through some mechanism of identifying those who don't.

But it is not an easy question, I know the Justice Department struggles with it and we are trying to come up with some answers in terms of a national I.D. And I believe a proper answer would probably come from someone who is on that group, who is looking at a national I.D. card.

Ms. NORTON. I am just looking for anyone on the panel that could tell how—I understand there is no policy yet and I don't expect you to endorse such a policy—I am trying to look for how effective this would be and whether it would eliminate more intrusive ways of trying to see if we are dealing with a legitimate party.

Mr. HOWARD. Congressman, I would be willing to answer part of that.

Obviously, as long as the government whether that is the state or Federal Government, is relying on paper documents which can be easily fabricated and fraudulent documents, it is problematic that we rely on those for authenticity of the person. And that is where the biometrics come in. Whether you relate that to a national I.D. card or some other type of identification that has either fingerprints or something else on it that allows for a match-up of that person to the card with that print on it goes a long way.

One analogy is the FBI's National Crime Information Center, NCIC, which runs millions of requests, of records checks if you will, both criminally and civilly from around the country, around the world, every year. There is a standardized protocol for submission to fingerprints to NCIC, so in other words, if your fingerprints aren't submitted properly, they won't go in the database. So there is a benefit of having standardized, uniform policy and protocol for submission of information on a national basis, and as an analogy, there is a benefit from doing that.

Mr. KISER. Mr. Chairman.

Chairman COX. Mr. Kiser.

Mr. KISER. Congresswoman, AAMVA's perspective is that the national I.D. is probably not needed. One of the by-products of a national I.D. is the creation of an infrastructure to actually issue one. And we believe that the infrastructure to issue I.D.s is in place in the state DMVs.

As we said earlier, there are loopholes and weaknesses in that process and we think that the appropriate approach is to strengthen what is already there and build on what is there and enhance it for the 21st century.

Chairman COX. I would also add that I wrestle with these same problems like all members, it may be that the Federal system is our strength here because one of the great fears that people have about the national I.D. card is that it will become the means and the basis for a central government repository of all information about you as an individual. Whereas if we decentralize the issuance of identification, that is less likely to happen. It is a big question and happily not the topic of today's hearing. Mr. Shadegg is recognized next, the gentleman from Arizona, for 5 minutes.

Mr. SHADEGG. Thank you, Mr. Chairman.

I think it is a perfect segue for some of the questions I want to ask. I am fascinated that the last answer says, "Well, we don't really need a national ID card because we have all these different DMVs and that is the vehicle to use," except that at least two states have already decided now to issue driver's licenses to noncitizens.

Both California and New Mexico are taking that step. It is being voted in my home state of Arizona. And I think there is legislation about to be introduced here in the Congress addressing that issue from a national perspective.

And I guess my first reaction was, well, it is none of the Federal Government's business to tell a state that they can't issue a driver's license to whomever they want except when I listened to the testimony as it was presented here today, talking about the importance of identification document fraud and then fraud involving state driver's licenses, it seems to me maybe it is the function of Federal Government.

And I introduced and was successful in passing the first Federal identity theft legislation. And I think this is a critically important topic. But to focus on homeland security, Mr. McNulty, if you were advising, say, the governor of Virginia on the issue of issuing driver's licenses to noncitizens, would you advise him against that for homeland security reasons or for it, or is it a mixed bag?

Chairman COX. Would the gentleman yield for just a moment, because there is some space in between the question and the answer for further refinement.

Does the gentleman have in mind noncitizens or people who are in the country illegally?

Mr. SHADEGG. Well, my thought is about people who are in the country illegally. But I assume we are already issuing some to noncitizens who are resident aliens with proper identification.

Mr. MCNULTY. Right. Right. That is an important distinction. I think that identification cards in Virginia and driver's licenses can be issued. But I would defer to my Virginia colleague here on that. I am pretty sure that they can be issued under the right circumstances. And, obviously, to get into the question then of issuance of identification to individuals who are undocumented, that is a whole other story and certainly creates new problems from the law enforcement perspective and an opportunity for individuals to, as I said, my testimony establish, legitimize their presence here for whatever purpose there might be.

So I probably should defer to Mr. Carico, whose office actually would find itself advising the governor of Virginia, as opposed to the U.S. Attorney. But I will say this just before I defer.

Our perspective that the validity of this form of identification, driver's license or identification card, is so critical to so many things. It just becomes the instrument by which people move about in the Commonwealth of Virginia, that our concern, of course, is that it is a very secure form of identification and that it is only given to those who have the proper place, that is, they are permitted to be doing the things they are doing with it.

We don't know what the hijackers did with their Virginia identification cards. But presumably, they used it to just establish their presence better. And that becomes a problem whether it is in the hands of individuals whose presence is not even legitimate or lawful in the first place. But let me defer to my Virginia colleague on that.

Mr. CARICO. Congressman Shadegg, in Virginia right now, under the new laws that we just passed in the wake of 9/11, we added a legal presence requirement in our laws so that people who want Virginia driver's licenses or state identification cards have to prove legal presence as well.

Now, there are many different statuses of people who are in the country who are not necessarily citizens but, like you said, resident aliens, there're people here under refugee status, temporary protective status, they are here on visas and the like, and with the Virginia law right now, those people can be issued Virginia driver's licenses or state identification cards if they have documentation that proves that they are here legally in the country.

Mr. SHADEGG. And Mr. Verdery, from the homeland security perspective, what happens to the validity of the driver's license if, in fact, the states can make differential determinations as to who gets them and if Virginia requires some proof of legal status and the states of California and New Mexico do not, for example.

Mr. VERDERY. The concern we have is more on the security side in terms of do you believe that the person who is getting the document is who they say they are, and then can that document be

used for various purposes to gain access to something that they are not qualified to do?

I do not believe the administration has a position point square on the issue of should illegal aliens be given driver's licenses by any particular state.

Our concern at Homeland is: Does anybody have access to an ID card that they should not have either because they are not qualified for it, or because they are an impostor, and that does lead them into situations that we would be concerned about, whether it is access to Federal buildings, access to airplanes, you can go down on the list.

Mr. SHADEGG. I just want to make sure I understand.

The Department of Homeland Security and in your view the entire administration has no view on whether or not the states should issue driver's licenses to people in the country illegally? Homeland Security has no opinion on that?

Mr. VERDERY. I am not aware that either the Department or the administration has taken a particular position on that exact question.

Mr. SHADEGG. It seems to me the Department's going to have to take a position pretty quick. Because, as my colleague from the District of Columbia pointed out, we all struggle with this issue of a national identification card.

I think surely that, as the testimony here today suggested, the American driver's license issued by one of the 50 states is what we are using now in lieu of a national identification card.

I have grave reservations about a national identification card. But if the standards for issuance of a driver's license can vary as greatly as the state of Virginia require proof of legal presence in the United States to get a driver's license, but the states of New Mexico and California do not require even proof that you are legally in the country for the issuance of a driver's license, it seems to me the driver's license then becomes not what it has been as a standard for identification in this country, and particularly if you look at what it is it takes in different states to get a driver's license.

My time has expired. But I think you are asking the same question I am in a different form. The way of making the driver's license secure, it appears to me, in most states has now been substantially differentiated from in at least two states where we no longer have control of the documents in even basic sense over what it takes to get a driver's license.

Chairman COX. Before I yield to Mr. Andrews for questions, I just want to understand the answer that the Department just gave concerning whether or not states should issue driver's licenses to person who are in the country illegally.

The Department of Homeland Security is responsible for, among other things, the Border Patrol. As we discussed earlier in this hearing, under United States law, citizens traveling in the Western Hemisphere can enter and exit our country by displaying a driver's license.

If the Department has not any view on whether or not people can be issued a driver's license when they are not legally allowed in the

country, then what in the world are we doing accepting this at the borders?

Mr. VERDERY. Well, I am not even sure it is actually accepted at the borders as proof of U.S. Citizenship. I mean, I understand the legal test that the inspector that somebody would run into at a point of entry has to be convinced that the person in front of them deserves entry to the country. They do not have to show any ID. It is entirety of the circumstances kind of test. A driver's license currently is seen as a good indicator that the person should be allowed back in the country.

Chairman COX. And if in fact, that is the practice, how is it that we can be completely without a view on whether people should be able to enter the country with a driver's license that we know is issued to people who aren't allowed in the country?

Mr. VERDERY. I think it depends on the totality of what we think the states are doing in terms of driver's licenses. As was mentioned in the testimony, some states such as Virginia, have tightened up their security features that are necessary.

Chairman COX. Will the department not accept California driver's licenses for California citizens across the border any longer?

Mr. VERDERY. I don't believe there has been a position taken on that.

Chairman COX. Well, this is all, it seems to me laid deeply at the feed of the Department. We hope to have some answers very soon on this.

Mr. SHADEGG. Will the chairman yield?

Chairman COX. Well, the time belongs to Mr. Andrews. With unanimous consent, I would extend the gentleman additional time.

Mr. SHADEGG. Mr. Chairman, can I just elaborate on one point just very quickly.

Chairman COX. Yes.

Mr. SHADEGG. A reminder that technically under the law, the driver's license is not proof of citizenship, and that Customs and Border Protection does not treat it as such.

Chairman COX. So technically those seven hijackers who obtained the driver's licenses from the State of Virginia before they attacked the World Trade Center and the Pentagon, and so on, weren't supposed to get them either.

But that is the purpose of today's hearing.

Mr. SHADEGG. Now, Mr. Chairman, in light of that followup, I would like unanimous consent for about 20 seconds to just follow up on the point that was just made.

Chairman COX. By all means, without objection.

Mr. SHADEGG. You just said that technically it is not allowed as proof of citizenship? I crossed the border into Canada twice this summer, and it was the identification I was required to produce, as was every member of my family.

So in theory it may not be accepted as admission, or as proof of citizenship to get in and out of this country, in practice it happened to me less than two months ago.

Chairman COX. Well, I think to be fair to the witness, what he said is that it is discretionary. 8 CFR 235.1 (b) says that you have to establish to the examining officer's satisfaction that you are a citizen and have a right to enter the country, and it is the case in

practice that that test is being met by presentation of a driver's license.

Hence today's hearing. You have been very patient. Mr. Andrews has the time for 8 minutes.

Mr. ANDREWS. Thank you. Mr. Chairman, I thank the witnesses for their participation of testimony today. The record before us is overwhelming that it is relatively easy for a terrorist to pose as someone else, and the impact of that is that the Integrated Watch List, other databases that the department is collecting and sharing with various agencies, is ineffective if we are not identifying the person who claims to be the person.

It is my assumption that biometric technology has progressed to the point where at least in most cases it would solve that problem. You can't use someone else's iris, you can't use someone else's fingerprint, you can't use someone else's biometric characteristics.

Does anyone on the panel disagree with the proposition? Putting aside for a minute the question of which agency should administer this, and how it should be paid for and by whom, does anyone disagree with the proposition that every driver's license and similar document in the country should have a biometric identification feature to it? Does anybody disagree with that proposition? Mr. Kiser?

Mr. KISER. Congressman, I don't disagree with that. A biometric identifier is a great place to be and we should be trying to get there, and in AAMVA we are trying to get there.

But we have had a two-year study of biometrics, and our conclusion at this point is that although biometrics works great on a one-to-one match, it is awfully hard to find the technology that works on an one-to–300 million match, which is really what we need to do to have an effective biometric identifier at this point.

Mr. ANDREWS. But doesn't that really get to the point that biometrics are not yet perfect, but they are clearly better than the piece of paper with your name typed on it. I mean, is there any serious dispute about that?

Mr. KISER. Not from AAMVA's perspective, no.

Mr. ANDREWS. I am not a professional the way you folks are on this, but I look at the situation this way. You have all told us, and I was particularly impressed by Mr. Malfi's report about how easy it was to get into Federal buildings and across the border with these fraudulent documents.

You have made it quite easy for a terrorist to pose as someone else. We have developing technologies that would make it a lot harder to pose as someone else. You could still do it, but it would make it a lot harder to do.

That seems like a no-brainer to me, that it should become the law somehow, whether it is by requiring states to meet this standard, or having one national entity that takes care of this, but we ought to do this.

I mean, am I wrong? Am I missing something here?

All right.

[Laughter.]

Assuming I am right, which I occasionally am, what recommendation would you make to the committee as to how we should implement such a change? Should we create uniform standards that each state jurisdiction must meet and then subsidize the

states rising to that standard? I don't think this cost should be visited upon the taxpayers of the states.

Or should we adopt a national system where driver's licenses and birth certificates and such documents are issued by the Federal Government? Which of those two should we pursue? And if there are other options, what are they?

And I would open that to the panel.

Mr. HOWARD. I will just make an observation. Obviously, the Justice Department will have a position. But I think one of the observations is, certainly as a citizen, is that, you know, when I was starting to drive, they went from a state being able to set its own speed limits to having everybody drive 55.

And what the Federal Government did at that point was that if you comply with the 55-mile-an-hour speed limit, then you can opt in to certain Federal funds. And if you didn't, you didn't get it.

I mean, money is always an incentive. I think there is certainly a concern in some quarters about a national identification card, but the comment was made earlier about having something like a driver's license, having certain information, certain qualities to it that would make it sound, make it something you could trust. And maybe a money incentive is one way to do it.

Mr. ANDREWS. Mr. Howard, as the chairman alluded to earlier, I think we are all instinctively reluctant to impose mandates, and we prefer incentives and suggestions. But this is one area where I would be for a mandate. It is inconceivable to me if we have the technology to make it more difficult to pose as someone else, that we don't require a way to do it. Again, I think it shouldn't be federally mandated and state funded. I would be in favor of us paying for it, if we are going to mandate it.

Mr. HOWARD. Again, Congressman, mine is just an observation.

Mr. ANDREWS. Yes. Anybody else care to recommend how we go about doing this?

Mr. VERDERY. One thing to keep in mind is that there is not necessarily the requirement that it be one size fits all, or that we have to have one master form for how documents might look. The trick is to have some type of security feature that we feel confident in, that is acceptable across the board.

The driver's licenses themselves or IDs don't have to look alike or have the same information. It is the fact that we want to have confidence that the issuing party, the DMV usually, has verified in some way that this person is who they say they are.

Mr. ANDREWS. I also understand that we don't want to freeze the technology in 2003. We want to be able to build in continuous improvements in biometric technology so it works better and better and better.

But, you know, I am as much of a civil libertarian as anyone here, and I don't want the government spying my affairs and knowing things it ought not know. But it seems to me that if I want the privilege of driving down the roads, or availing myself of other public services, requiring me to show that I am who I say am is not at all an intrusion upon one's liberties and it is something that we ought to just make happen.

Not to say this in any accusatory tone to the Secretary, but I think it is disheartening that we are 25 months now away from this calamity and this situation still exists.

And I respect our Federalist traditions. I understand that this is expensive. I understand we shouldn't rush into a solution without understanding the technology of it, but we have to get on the stick here.

And I commend the chairman for calling the hearing. I think that we need to get the best minds in the country, which you represent, together and tell us how to fix this problem. I think we have spent $74 billion on homeland security since September 11th of 2001. Some of that should have gone to this, and the next piece of it will certainly go to this as well.

So I thank the witnesses for their testimony and the chairman for his wisdom in calling the hearing.

Chairman COX. The gentleman from Connecticut, Mr. Shays?

Mr. SHAYS. Thank you, Mr. Chairman.

I am somewhat reluctant sometimes to get into the issue of illegal immigration, because sometimes it has a connotation to people.

But I wrestle with this, like probably all of you do. It is illegal to be in this country, but we find every way to accommodate people who are here illegally. We give them driver's licenses. We allow them to register with banks. We know they are here illegally, and we turn the other way.

I would double legal immigration, but we have about 8 million people who are here illegally and we don't seem to know how to address it. And what I am wrestling with right now are the rules done by Treasury, and I want to know each of your opinion about it.

And what we did in the PATRIOT Act was we basically said we wanted Treasury to establish verification so that we could get at money laundering, et cetera.

So they basically came out with their rules and they came out with their rules in July, and there was such an uproar in Congress that they did an inquiry and decided that they would look at it again, and then when there was the storm and the government was closed down, they came down and reaffirmed that they were going to keep the same rules.

And the same rules basically say the final rule provides that for non–U.S. persons a bank must obtain one of the following, a taxpayer identification number, Social Security number, individual taxpayer identification number, or employer identification number, passport number and country of issuance, alien identification card or number, and country of issuance of any other government-issued document evidencing nationality or residence, and bearing a photograph or similar safeguard.

First off, I would like to ask each of you, can you have a fraudulent taxpayer identification number?

Let us start with Homeland Security.

Mr. VERDERY. I am not sure I understand the question.

Mr. SHAYS. All right, let me give you an easy one first.

Chairman COX. Actually, if you would let that question hang out there and be answered, and let me just qualify it. If I understand your question, it is is the taxpayer identification number a reliable

basis for the issuance of identification? Or is it a reliable basis for anything?

We have covered this in this hearing already. I think that is a pretty easy answer. Hopefully, you don't have any question about it on the panel.

Mr. SHAYS. Well, let us go right down.

Mr. VERDERY. Well, I think the Treasury Department and their regulation says that it is for purposes of these banking issues.

Mr. SHAYS. I don't care what they think. I want to know what you think. Let me say to preface, you are in charge of homeland security. They have a perspective, you have a perspective. And I want to know your perspective. And having had 5 years of hearings on this kind of stuff, it is hard for me to smile anymore about it.

Mr. VERDERY. Well, as the chairman mentioned, I believe, in his remarks earlier—

Mr. SHAYS. I don't want to know what the chairman said; I want to know what you think.

Mr. VERDERY. Well, there are concerns about requirements or identification criteria such as the ITN that we are not sure that the person who has it is who they say they are, but the Treasury regulations make clear that—

Mr. SHAYS. Why are you taking the time telling me—I just want to know what you think. Is it a reliable document? It is, yes or no?

Mr. VERDERY. It is reliable in some cases.

Mr. SHAYS. And in other cases it is not.

Chairman COX. Will the gentleman yield? I mean, you know, the people who manufacture these numbers, the IRS, have the following to say about it: "Taxpayer identification numbers are strictly for tax processing. We do not apply the same standards as agencies that provide genuine identity certification. ITN applicants are not required to apply in person. Third parties can apply on their behalf. We do not conduct background checks or further validate the authenticity of identity documents. ITN's do not prove identity outside the tax system and should not be offered or accepted as identification for non-tax purposes."

I can't imagine anything more clearer than that. That is what the IRS says and they are the ones who manufacture the numbers. So to have the Department of Homeland Security say maybe they will be good sometimes, then I think we have a big problem here.

Mr. SHAYS. I would like you to respond to what you just heard.

Mr. VERDERY. Again, this has gone through an interagency process. The Treasury Department has issued regulations that have been approved by the administration and—

Mr. SHAYS. You know what you are saying to me? You are telling me how it happened. I have been in Congress 16 years, and I want to know what my Department of Homeland Security thinks, and the reason I want to know that is I helped establish this organization because I thought you might be a counter to some of the junk that we have seen come out of other departments.

I thought you might be focused on homeland security and protecting our citizens. So I want to know what you think and what your head thinks. I want to know what you think. I don't want to know what you think someone else thinks.

Mr. VERDERY. The Department weighed in on this during the interagency process.

Mr. SHAYS. And said?

Mr. VERDERY. And expressed concerns about the regulation in general. And the administration made a decision that the Treasury regulation would go forward.

Mr. SHAYS. Right. But the answer to it is, the Department disagreed with the decision. There is nothing wrong with saying that. You heighten, frankly, and make me feel a little better about the department. The position was you opposed it, correct?

Mr. VERDERY. There were certain things about the proposed regulation we had concerns about, yes.

Mr. SHAYS. And wouldn't one of them have been based on the very explanation you heard from our chairman?

Mr. VERDERY. About the parts of the regulation that we thought were not as—the documents that would be accepted that weren't as secure as we might like.

Mr. SHAYS. Mr. Pistole, how many times have you met with Mr. Verdery?

Mr. PISTOLE. None.

Mr. SHAYS. None?

Mr. PISTOLE. None.

Mr. SHAYS. This is the first time you two have met?

Mr. PISTOLE. Yes.

Mr. SHAYS. Why?

Mr. VERDY. Well, I was just confirmed a few months ago.

Mr. SHAYS. OK.

Mr. PISTOLE. If that answers the question.

Mr. SHAYS. How many months ago?

Mr. VERDERY. I guess three, two or three.

Mr. SHAYS. So this is the first time you all have sat and talked about this issue?

Mr. PISTOLE. Yes.

Mr. SHAYS. What do you think about a taxpayer identification number?

Mr. PISTOLE. Really, it is an unreliable form of identification for verifying the authenticity of the person. And by way of analogy, several of the 19 hijackers when asked to provide a Social Security number simply wrote a number in a document form that was not verified. So anybody can fabricate a number if it is not verified for authenticity.

So we have concerns, have expressed those concerns both in that regard and also from the standpoint of the perhaps inconsistencies in the way that they may be scrutinized. So even if there is a legitimate taxpayer identification number, or Social Security number, if the entity, whether it is a financial institution or otherwise, is not exercising due diligence in scrutinizing that number, then it is to no avail.

Mr. SHAYS. How about, if you would respond to this, the number and country of issuance that any other government issued document evidencing nationality or residence and bearing a photograph or similar safeguard?

What do you think of that, Mr. McNulty? Mr. McNulty, I am—excuse me, Mr. Pistole, I am sorry.

I am sorry. I am so eager to go through this. Why don't we take the first one and just do—I think we kind of know the taxpayer number, but why don't you respond, if both attorneys would respond?

Mr. MCNULTY. All I can say as a Federal prosecutor in Virginia is I have prosecuted people for using a stolen taxpayer identification number, or a bogus tax identification number. So, obviously, it is another form of identification that is subject to theft and fraud, and it is not reliable therefore in some kind of means for establishing positive identification in the way we are discussing today.

Mr. SHAYS. Thank you.

Mr. Howard?

Mr. HOWARD. I would agree with that. I think that unless you are going to do the background to it to find out who actually filed the taxes, where they were filed from, verify a signature, if all you are going to do is present the number, it is certainly our experience that almost any number can be fraudulently obtained or manufactured.

Mr. CARICO. Sir, in Virginia, we do not see the tax identification numbers as being reliable enough to allow for someone to, like, get a driver's license or state identification card. So my answer to you would be that we in Virginia do not find that it is reliable enough to get those sorts of identifications.

Mr. SHAYS. Thank you.

Mr. MALFI. From the operations that we conducted, part of the problem is that cards or pieces of identification that are issued by the government, or by the state, gives people that are examining them a false sense of security and almost a complacency for the fact that if you have one of these cards, which they really have no way to validate the authenticity of them, it lets their guard down because they feel that because you are a bearer of this instrument, or this document or this card that is issued by a state or a government, that you are who you are.

And the important part in regards to all of these types of documents is that, one, they are issued for different reasons, and we can't have a document that is being used for something other than what the original purpose to issue that is.

Mr. SHAYS. Thank you. Very helpful, gentlemen.

And, Mr. Chairman, I know my—I realize, but let me just proceed.

Yes, sir?

Mr. KISER. Congressman, we believe that the ITIN, or the taxpayer identification number should not be used as a breeder document in the issuance of a driver's license.

Mr. SHAYS. So I guess we conclude, Mr. Verdery, you are supposed to be the champion of homeland security, you are supposed to be the one organization we turn to. And when we go right down the line, no hesitation, no qualification, no BS, just the realities of circumstance for members of Congress to then make a judgment. I would like to think that I could get that same precision from you and, frankly, from the Department.

Chairman COX. The gentleman's time has expired.

The gentleman from North Carolina, Mr. Etheridge, is recognized for 8 minutes.

Mr. ETHERIDGE. Thank you, Mr. Chairman.

Let me also join my colleagues in thanking you for this hearing and for all of you for being here. This is an important hearing today, and I hope that from this hearing we will find a way to find some legislation to deal with an issue.

I couldn't help but think as the dialogue was going on about how we use a driver's license. If I go out today to National Airport, or to Dulles, and decide I am going outside the United States, I am going to present a passport or I am not going. Now, I realize this is a little different. Even if I am flying to most any place, Canada, Mexico, otherwise, I have to present a passport and when I get there, they are going to ask to see it.

Now, I am not sure I am going to get that far with a driver's license, but the point is that if we do that for air travelers, then we don't deal with it on the people who get on our roads and drive from point to point, we would never have worried about if we hadn't had 9/11. This is a serious matter.

One other point I will make and then I want to ask a series of questions. You know, we have a lot of Federal, state and local partnerships. We do it through transportation systems, we provide monies for highway transportation, the interstate system, secondary roads, et cetera. That's a partnership.

And to get that money, you have to meet a certain standard. I know. I served as a state legislator and as a county commissioner and as a statewide elected official. You do not get that money until you meet that standard.

And yet, here we are talking about an issue that is critical to our national defense and the security of our people, and we cannot seem to agree that we ought to have a standard from state to state.

So with that, let me ask a couple of questions.

How is the Federal Government working with state and local officials to provide information about identity theft?

And I guess I ought to start with you, Mr. Verdery, since you are Homeland Security.

What are we doing to help with this issue? Because it is obviously quite serious.

Mr. VERDERY. Well, as I mentioned in my prepared testimony, there is a number of different things going on. And I suppose it would be nice if they were all centralized in one place.

But there are a number of agencies that have responsibility in this area. The Secret Service is working quite a bit with state and locals in terms of trying to get out the word on identity theft, how to prevent it.

You have the Secret Service working with AAMVA on driver's license issues, trying to develop security standards. We agree with them that there should be a unified standard for the issuance of cards in the security standards.

You obviously have the prosecutions for identity theft both by our Federal agents at ICE and Secret Service but also down at the local level with our prosecutors. Not to mention the efforts more on the civil side with the Federal Trade Commission, which has a

huge outreach effort to combat identity theft under Chairman Muris.

I mean, there is a lot going on. Is it as much as we should be doing? Perhaps not. But there is a lot of work going on to try to develop security standards in this area.

And again, I would not want the record to close today without returning just briefly to the work we are doing on passports and foreigners trying to come to this country on passports and visas. Over the next couple of years, things are going to change quite a bit in terms of biometrics being incorporated in those documents.

If we are worried about terrorists coming in, especially on airplanes, it is going to be a lot harder for them to find a way into this country without being checked with various watch lists and the like.

Mr. ETHERIDGE. Well, that was not the point of my statement as it related to passports. The point of my statement with passports was the fact that we have pretty good security if I am going to fly. The question is, we are talking about identity theft and we are allowing our driver's license to be one of those issues that opens the door for a lot of opportunities.

That being said, let me follow up with this question—and I am not trying to pick on you, Mr. Carico from Virginia. It just happens other states are doing some of the same things.

But it deals with the whole issue of having an identification number on a driver's license. And in the case of Virginia, obviously, I believe you indicated they use the Social Security number on the driver's license. Is that correct?

Mr. CARICO. No, sir. No longer.

Mr. ETHERIDGE. No longer. You did do it, OK. +

I think there are some states that still do, so let me follow that up and get you to respond to that. Because the Social Security Administration and others have indicated that that is one of the issues that they are concerned about, and they discourage that as much as possibly simply because that opens up a whole new avenue of identity theft.

That being the case, did Virginia go to the random numbers in using the ID number?

Mr. CARICO. Yes, sir. We now have driver's license numbers that are assigned once you go and request a driver's license.

Mr. ETHERIDGE. Do you know how many states now use that system?

Mr. CARICO. I do not, sir.

Mr. ETHERIDGE. Can you enlighten us?

Mr. KISER. Congressman, my understanding is that all states now offer citizens the option to use some other number than their Social Security number on their driver's license.

I know that in my state, some citizens have chosen not to change their number, but they do have that option and are offered that option at the time they renew or at the time they raise the question.

Mr. ETHERIDGE. Well, let me follow that up, if I may.

So it is an option on the part of every state, or most states?

Mr. KISER. All states, as far as I know, sir.

Mr. ETHERIDGE. It's an option.

Mr. KISER. Yes.

Mr. ETHERIDGE. So if we want to prevent identity theft, it seems to me that that would be one way to execute that.

Mr. KISER. Congressman, I think you are absolutely correct.

And again, in the case of my own state's experience, most citizens have chosen to take a randomly issued number. But some have in fact asked to have their Social Security number left on their driver's license, for whatever reason.

Mr. ETHERIDGE. Mr. Verdery, let me come back to you then, we are talking about identity theft, we are talking about homeland security, helping to protect the homeland, and this being one of those areas that can open up a lot of Pandora's Box.

What is the Department doing to discourage the use of Social Security numbers on driver's licenses? It would seem to me this is an area that we can have some impact.

Mr. VERDERY. Well, I am not aware of particular efforts in terms of our discouraging states from using the numbers themselves. I know we are working closely with the Social Security Administration generally to try to figure out ways to tighten up the use of those numbers across the board.

But I am not aware of particular efforts in terms of trying to get the numbers off the ID cards themselves. But perhaps that is something that should be looked into.

Mr. ETHERIDGE. It would seem to me that is part of what homeland security is all about. If you are getting it off public documents, you are saving an awful lot of time for the rest of the folks sitting on this panel and the American public at large.

So I would hope that would be something you would take away from here today, and spend some time on. It seems to be a good use of time.

Mr. Kiser, what training are state DMV workers receiving at the present time to help identify false documents? And how should, or could, this training be improved to reduce the issuance rate and the problems we now face to validate and get the identification right?

I know we have talked about a lot of the issues. It seems to me the first issue is training until we get some legislation to deal with the other two, to save some of the problems we are having in identity theft.

Mr. KISER. Congressman, AAMVA's worked on a couple of fronts in that area. One is we have developed a standardized list of acceptable documents that should be used for identification purposes, or breeder documents, in generating a driver's license.

Beyond that, we have developed a fraudulent document recognition training program that we unrolled to our membership on a limited basis over this past summer, that we now have scheduled training for at least one representative from each jurisdiction over the next several months where they will get a five-day training course on fraudulent document recognition.

And how can that be helped? There is a cost to doing that. And so, you know, those costs are being shared now with AAMVA. I think we are getting some assistance from NHTSA, I believe, but to continue to fund that the effort is to train at least one person in each jurisdiction who can then go home and train additional DMV employees in the jurisdiction.

So that program is up and running. The reviews from its initial pilot were very good. It was expanded from three days to five days to address some additional issues.

Mr. ETHERIDGE. Mr. Chairman, thank you. I know my time has expired, but what you are talking about is train the trainer.

Mr. KISER. That is correct.

Mr. ETHERIDGE. And the key is how well that first trainer is trained. And I would hope, having had a little bit of experience in education, that we would use the issue of rewards in terms of a level of certification, because I know it takes money to get that to some point, but sometimes, given the challenge in this country that would be a great way to do it in terms of without a lot of additional resources.

Mr. KISER. Congressman, we are looking at a certification program that may enhance that employee's self-esteem, maybe their status within their jurisdiction.

Mr. ETHERIDGE. Thank you, Mr. Chairman.

Chairman COX. Thank the gentleman. The distinguished ranking member, the gentleman from Texas, Mr. Turner, is recognized.

Mr. TURNER. Thank you, Mr. Chairman. Mr. Verdery, I want to follow up on some of the sentiment that was expressed by Congressman Shays. It seems that we really need your department to be an advocate for greater security.

You know, we consider it our responsibility in oversight to try to close these security gaps, but it is disturbing when we learn about some of these and that the Department hasn't stepped forward and urged that these gaps be closed.

In your opening statement, the written version of it, on page one, you reference about one problem, that the current law allows a U.S. citizen to leave the United States and travel to any country in the Western Hemisphere, except Cuba, and return to the country without, showing a passport.

Now, it seems to me that if we are going to control who is coming in and out, the problem is simplified if we know who the good guys are. In this instance, if we knew that we were dealing with a U.S. citizen, if they had a passport that was presented upon leaving and re-entering, then that would help close the gap and solve the problem that you went to great lengths to describe in the first page and a half of your testimony. And yet, nowhere in that presentation do I see that you suggest that the Congress ought to close that potential gap.

These are the kind of suggestions and the kind of advocacy that I think we need from the Department. If you have a position on that, it wasn't expressed in this presentation. But it just seems like common sense would tell us that if it requires a passport to travel in and out of the country as an American citizen to go other places, that if we don't require it in the Western Hemisphere, that a terrorist can fly into Brazil and then into Houston and assert that they are a U.S. citizen. And they walk right in.

So there are some common sense things here that the department ought to be advocating to the Congress to it. You ought to be out front. You ought to be the leader. If it turns out it is too restrictive, that Congress rejects it or somebody thinks it is too burden-

some on the American people and we want to leave that gap open, well, we made the choice.

But why is it we don't have the Department coming up here and telling us we ought to deal with this issue that you so clearly articulate there in your own testimony?

Mr. VERDERY. Well, we are looking pretty carefully at the requirements for U.S. citizens as they return back into the country as we are working on the implementation of the U.S. Visit system which I mentioned earlier. Now, clearly, it is a problem as I outlined in the testimony.

Now, I think if you talked to colleagues on the northern border especially, people who are U.S. citizens who are used to going back and forth, out of the country to Canada, asking them to have a passport for each trip back and forth is something they are going to be very interested in.

But we are trying to weigh the equities here and try to figure out balance of security needs versus the economic needs. And it is something we are definitely focused on. At this point today sitting here today, I can't tell you that we are recommending solution X or Y. But it is something we are closely examining along with the State Department.

And in terms of your hypothetical about the person flying in from Brazil, that person has to go through a CBP inspector. Presumably, if he is from Brazil, the inspector hopefully is going to recognize that he is probably not a U.S. citizen and will require the type of passport control that you would need at an international airport. That is what they are there for. That is why we have gone 18,000 of them to try to distinguish between those people who need that kind of entry document and those who don't.

And while I have the floor, I realized from your remarks that my conversation with Congressman Shays may have left an unclear impression. The Department agrees that the ITIN does not in and of itself prove identity. The Treasury Department has decided, for purposes of banking regulations, that it can be used or can be accepted by financial institutions for opening up a bank account. But beyond that, we agree with you concerning other utility to establish identity with that kind of document.

Mr. TURNER. Thank you, Mr. Chairman.

Chairman COX. The Treasury was implementing changes that were occasioned by the Patriot Act. I mean, it is just sort of remarkable that legislation that was meant to make it easier to get after terrorist money was implemented in such a fashion that it opened up possibilities for people to fraudulently open bank accounts. Don't you agree?

Mr. VERDERY. As I have mentioned, we had various concerns with the regulation. It is now final. And we raised those concerns.

Chairman COX. Well, if it is a final regulation, it is certainly not final in the Capitol. And we are going to be after this.

We have heard today the full spectrum of crimes that are facilitated by document fraud and identity theft. I wonder, what about abuse and waste in, for example, government benefit systems?

We have two U.S. attorneys here. Possibly you can tell us whether the kind of document fraud that we have been hearing about

today contributes to abuses such as Social Security benefit fraud or Medicare of Medicaid fraud?

Mr. McNulty? Mr. Howard?

Mr. MCNULTY. Absolutely, Mr. Chairman.

These frauds sort of are layered, and they begin with fraudulent acquisition of some form of documentation. But it just takes off from there.

And the vendors of fraudulent documents are skillful at providing a variety of documents that will allow a person to engage in a whole fraudulent scheme or enterprise that they might need in order to achieve whatever fraudulent goals they have.

And so you have a terrible waste of resources at agencies spending time issuing these fraudulent documents.

Consider the Department of Labor alone, issuing thousands of fraudulent certificates for acquiring a job in the United States and the waste that is.

The amount of abuse of the proper role of these various agencies and what they are doing, through all of the different fraudulent schemes, is just staggering to consider.

So I think that from an abuse perspective, this whole problem of document fraud in trying to deal not only with the prosecution of the crime but reforming procedures so that the agencies issuing various forms of documentation and identification are really looking at how they are going about their business and how they are screening and analyzing the applications and other things that they are receiving would be an enormous benefit to our government.

If you could improve that, I think we could reduce this problem substantially.

Chairman COX. Mr. Howard?

Mr. HOWARD. Although you are talking about fraudulent documents, some people want to steal your identity. They want to be you. They want to take your credit, they want to be able get the great benefits of being a Congressman from California, so they want to be able to buy a house, buy a car, get credit cards, take vacations.

It is a different sort of issue, but if you talk about fraudulent activity, we estimate that people in this country are the victims of identity theft, probably about 33 million people, and certainly a number of them are here in Washington.

And it is a really a life-style change. You have got people who literally can't get their lives back. They can't, in their own good name, get credit because of what other people are doing.

So it is a huge issue. I think it is one of the reasons that the Postal Service has kicked off their Operation: Identity Crisis.

And one of the things we have learned, I think all the U.S. Attorneys have learned, is it is something we have to work together with on all law enforcement.

One of the things we are going to do in the U.S. Attorney's Office in the District of Columbia is just have training on, one, how to recognize it.

Certainly one of the areas I think that legislation can be used is, often the victims find that once they find they are the victims of identity theft, banks and other institutions make it up to them to

prove in fact that they did not commit these crimes. It really kind of turns it backwards, especially for someone who is going through one heck of a time trying to gather their good name back.

But it is a huge, huge problem in the District of Columbia and the country in general.

Chairman COX. The gentleman from Florida, Mr. Meek, is recognized for 5 minutes.

Mr. MEEK. Thank you, Mr. Chairman.

And I thank our panel for being here today. I just want to say as it relates to this identity theft and fraud and enforcement that is needed, I don't believe that the country is ready to do what it has to do for a national identification card. I really don't honestly believe that.

I for one am a past law enforcement person as it relates to Florida State Highway Patrol. I have been dealing with driver's license for a very long time now and I can tell you we can go, we can change the driver's license every 3 years. There is always going to be a way to get a counterfeit one.

As it relates to a national identification card, we talk about the Patriot Act I, there were those voices that were saying that we needed a Patriot Act I, once upon a time. Right now those same voices are saying we need to do away with Patriot Act I and definitely not do Patriot Act II if it is going to be the intrusion of civil liberties and individual right. And it is interesting to hear those voices say that.

I do believe if something does happen, God forbid, in the very near future in our country as it relates to safety or an event takes place in our country, an identification theft or fraud or something has something to do with that, then maybe we will be able to move some legislation at that time. But unfortunately that is going back to the traffic light situation of saying that we have to have X amount of lives lost before we put a traffic light there.

I want to know what is going on as it relates to the community that is sitting at the table. Obviously if each one of you individually don't get together under the light of Homeland Security, people in your agencies do. And how does that bubble up and bubble out and get up here on the Hill through the Department of Homeland Security, through the Justice Department, need it be through the FBI of recommendations on what we should do?

I have been a part of panels and I have seen it, I have watched C–SPAN, I hear folks talking about what we need to do and what we ought to do. But when the bottom line, the final analysis, there has to be a horrific event before we get down to moving the ball down the field.

And when we move in haste, these sort of things happen as it relates to banking, as it relates to what is going on with individuals that are not going through screenings and all of these things. So we need to be able to move forth.

The purpose of this hearing today, getting back to it, was about hopefully moving the Department in the direction of making sure that we are more aggressive, of moving in a direction that we need to move in. I

mean, I said it the last hearing that we got together, and the chairman is fully aware of it—and we have a vote coming up right

now—the fact that this time of calm waters that we are experiencing right now is not a time for me to say, "Are you OK, law enforcement community?"

"Well, I am OK."

"Well then fine, let's go have lunch." No, it is time for us to make sure that we continue to stay ahead of these individuals that are trying to hurt us.

I want to ask anyone on the panel as it relates to the carrot-and-stick approach. We talk about federalism, we are talking about states that are not following what the Federal guidelines are set out for. People around here are driving 55 and 65 because the Federal Government says they are going to cut highway funds.

Any discussion as it relates to what we can do to make sure that we move forth as a union, not as a half a union, but as a union toward these United States that I am talking about, towards safety of our homeland as it relates to our subject matter, distributing driver's licenses, not having that information that we need, any discussion on that or any thoughts or ideas? Anyone may add.

Mr. KISER. Congressman, there was an earlier conversation about the issue of state's rights and the carrot-and-stick approach. And I think it is a fine balance.

It is clear to me that the Congress, the governors, the legislators in the jurisdictions have to work together to come up with a solution that will work. We never believe that we have a large piece of that solution ready to roll out. It is not in our authority to do it. We need the Congress to advocate that there in fact is a problem and that there is a huge problem and to be an advocate for saying there needs to be better integrity.

You can tie that to the carrot-and-stick approach. That obviously has worked in highway funds and speed limits and all sorts of things in the past. And that certainly gets the attention of state legislatures and governors, for that matter.

And so, we believe we can solve some of these problems. As someone said earlier, and they are correct, that you will probably never prevent all of the fraud that occurs, but I do think there are things that we can do to bring the driver's license process into the 21st century. I think that the state administrators and DMV are ready and willing to do that.

Mr. MEEK. When you say bring it into the 21st century, are you talking about some sort of national seal on a driver's license? Are you talking about one particular driver's license? What are we talking about here, because I can tell you that the Treasury Department, as it relates to seals and paper and all of these things, they are switching to every 3 years. They are regenerating themselves, but they are finding counterfeiting is pretty prevalent.

Mr. KISER. We believe that in order to move to the 21st century, you have to have unified standards. The document may not look exactly the same from jurisdiction to jurisdiction, but it should have a set of standard security features. It should have placement of data in a particular position so that it is recognized by a law enforcement officer or an airport worker or whoever that might be. And so, yes, we do think that there needs to be a great deal more standardization of the document itself and the contents of the document in order to enhance that security.

Mr. MEEK. Last question, Mr. Chairman.

Chairman COX. I see the gentleman's time has expired. And I really need to be punctilious about this because we have two members on the Democratic side and we are running out of time on the floor.

And I don't know who I am supposed to recognize next.

Ms. Jackson Lee, the gentlelady from Texas, is recognized for 5 minutes.

Ms. JACKSON LEE. I thank the chairman very much and apologize to the witnesses, overlapping hearings that have been occurring, that I did not get a chance to hear all of your testimony, but I certainly have perused a good deal of it.

I served as a ranking member on the Immigration Committee, on the Judiciary Committee, so some of these issues we have dealt with, particularly the issues dealing with the use of the biometric card or the use of various identities as it relates to immigrants. And, of course, we have had hearings on the matricular card as well.

But let me focus on where I would like to go with this, is the question as to what would be the best vehicle to ensure that you have the tools to make sure that America's homeland is safe. I think you are entrusted the responsibilities of law enforcement, but you are also prevention as well, because when laws are passed, when they know that there are strong oversight provisions and oversight institutions, then people are hesitant to engage.

First, I would like to say that I am on record for being opposed to a national identification card. I don't think that it is going to be advantageous, because any unified document is subjected to even more opportunities for fraud because you become familiar with it. And it becomes a document that you can then make more perfect—the ones who are perpetrating fraud. The tax ID numbers have been fraudulent as well.

So let me raise these questions. And I would appreciate it if you all would answer it.

What would more training do, more staffing do and more technology do for all of your work? Is that where we are going? I know there is a bill, Paul—if I might the U.S. attorney that, having served with him on the Judiciary Committee.

There is a H.R 1731. And if you recall, I am not sure if you had left the Judiciary Committee. We did something on identity fraud when we had that horrible experience of FBI agents going into the Department of Justice about, maybe, 2 or 3 years ago with false documents. I guess that was part of the overall study. We had hearings in Judiciary. And it wasn't dealing with terror and immigration as much as it was dealing with people violating the sanctity of secure areas.

So would we and could we do a better job if we said to the various U.S. Attorneys' offices that are represented, Mr. Howard and Mr. McNulty, that we gave you more resources and a separate unit that dealt only with ID fraud? And then others may want to pipe in as well in your respective areas. But if I can to my two U.S. Attorneys on that, I would appreciate.

Training—because I know I need to give more training to my immigration inspectors, clearly need to give more training to them.

How would that help in your preventive and prosecution work?

Let me finish my sentence by saying even as I am supporting us doing a better job with determining identity fraud because I know that helps secure the homeland, know that I am also facing every day the insults and confrontations by those with Muslim backgrounds or Arabic last names, individuals who come to this country repeatedly to do nothing but good or to use our medical services and are treated in a horrific way. And they have good documentation. So I want to make sure that I am on record for balancing, protecting the homeland and respecting the dignity of individuals coming into this country.

I would ask the two U.S. Attorneys and then others, if they would, if we have the time.

And thank you.

Mr. MCNULTY. Thanks for the question.

There are two things I would identify that would help a lot. First, authority to enforce various provisions of Federal law. One of the problems we run into is that among the various Federal law enforcement agencies, they have jurisdiction for particular statutes, particular types of identification fraud. And unless you have them together in a task force, you have a problem of identifying one category of fraud that leads to others but not having the right law enforcement agency present.

So one of the things that I think would help, especially with homeland security if I could speak for Mr. Verdery, is that as they stand up and organize the jurisdiction and the responsibilities of ICE and the other entities, that the authority they have to go after identification fraud be expanded so that they can address various frauds at the same time.

For example, Social Security fraud is connected closely to various forms of immigration fraud. Now, the Social Security Administration has jurisdiction over Social Security fraud. I am sure they would welcome the help of Immigration and Customs Enforcement, ICE, in investigating those kinds of offenses.

second, when it comes to resources, while I am not in a position to be able to go around OMB and ask for more money for the administration, I will say this: that the more immigration investigators we have, the more we can do in this area. Our task force has brought together 14 or so agencies, including local police departments, to go after immigration and visa fraud. It has been very effective to pool those resources.

But we certainly depend particularly and primarily on ICE. That is the agency that has the lead in this area of immigration fraud investigations. And to the extent they have the resources to match them up with U.S. Attorneys' offices and the task forces that we are creating, we will be in much better shape.

Mr. HOWARD. And I will echo that, Congresswoman. And, you know, if I can take them in order, first of all with training, I can't agree with you more. One of the things we do in our office is we have a bias crimes task force for some of the issues that you have. A lot of times I think AUSAs, as honorable as we are and as hard as work, sometimes we don't understand the issues that an immigrant community may be seeing that we don't. And so what we

have asked them to do is, we have asked them to come into our office and educate us.

One of the ways that has helped us is we have actually been able to recruit some AUSAs off of that, so it has really helped us. But we in turn use that as a vehicle to go out into the community and then educate the community about what the issues are, sometimes what we are doing out there, and then who it is you call.

And so training very, very important. But that is something we pull out of our budget, and clearly when we pull that out of our budget, then, you know, I am taking away from something else that we think is important.

Resources. Certainly resources, I am like all AUSAs, if somebody suggests resources, yes, you know, we can do more with more U.S. Attorneys, assistant U.S. Attorneys, but also for, as Paul said, INS and the FBI.

Clearly, the FBI is being asked to do an awful lot in terrorism, and I think that more agents in both areas would allow them to dedicate resources. One of the issues we find in the Adams Morgan area is that we can go in and we can take out these mills, but we can't be up there 24 hours a day, seven days a week. They simply have other duties. As soon as we move away, my guess is it takes them a good 15 minutes to have somebody fill that void.

We are back there. We have to do surveillance. It takes us a while to build the case and we identify who exactly the cancer is so we can pull it all out. But we pull them out in groups of 15, 20 and 25, and somebody is back in there. And so resources just to address the problem is very helpful.

And then you said equipment. And a lot of times—

Chairman COX. I wonder if I could ask you to summarize—

Mr. HOWARD. Sure.

Chairman COX. —because we really do want Ms. Slaughter to be able to ask her questions and we do have a vote on the floor with just a very few minutes left.

Mr. HUNTER. With equipment, I say ditto. How's that?

[Laughter.]

Chairman COX. That was an outstanding summary, if ever I have heard one.

Chairman COX. The gentlelady from New York.

Mr. VERDERY. Mr. Chairman, if I could have 20 seconds in response to the Congresswoman's question about the training?

Chairman COX. I just want to make sure that Ms. Slaughter gets a chance to ask her questions, and then there will be endless time for you all to speak for the record.

Ms. SLAUGHTER. I thank you, Mr. Chairman. It is really important to me to do this.

Gentlemen, I represent 100 miles of the U.S.–Canadian border, and we are very concerned up there with the fact that we are not getting what we need for first responders.

And since I am not going to have much time, Mr. Verdery, I want to really address this to you, and I am going to cut right to the most important part, although everything I am doing is important.

Now, I know this is not within your purview, but you are the assistant director there and I want you to get the answer for this and get it back to me. OK? All right.

Niagara Falls, New York, applied for one of the DOJ grants for overtime for police. And Niagara Falls, New York, as you know, not only represents one of the largest power plants on the face of the Earth, one of the seven wonders of the world, but towers and all kinds of trestles to carry the electricity across the state of New York, international railway infrastructure and over 5 million visitors a year, and they didn't get one.

Now, one of the reasons maybe why they didn't get one is New York got 13, 13 of those grants.

Chairman COX. If the gentlelady would yield, I just want to let her know that there is less than a minute left in the vote on the floor.

Ms. SLAUGHTER. All right, thank you. You all go vote, this is more important to me, I think, than this vote.

Chairman COX. Except that I have got to adjourn the hearing before I can go vote.

Ms. SLAUGHTER. Oh.

Chairman COX. So what I would suggest is that you put your entire question on the record, and then we will get it answered for the record.

Ms. SLAUGHTER. All right. I have a couple more questions and I will put them in as well. But anyway, New York State, as I was saying, got 13, Puerto Rico got 155.

Now, there is no earthly reason why Niagara Falls, whose costs have more than tripled, would be, this is a case of really rural counties, farm counties, in the State of New York that got these overtime grants on homeland security.

I agree with the GAO. This grant idea really has got to be reformed. It doesn't make any sense.

We do not have unlimited resources here, and unless there were political considerations involved, I cannot for the life of me understand why a place as strategic as Niagara Falls, one of the most important border crossings in the country, with everything else that I have mentioned, and in addition numbers of chemical plants and remnants of the Manhattan Project, I almost hesitate to mention the targets that are there in that one small area.

But to not get any attention at all, and certainly not to get any help when they were paying overtime, it absolutely makes no sense to me.

As their representative, I am as mad as I can be about it. And I want an answer, and I want it as soon as I can get it, and I want to see what we can do to remedy this, because there is no way they are going to be able to try to even continue what they are doing if their costs are tripling and quadrupling.

And there is no help, and those costs are incurred because of what they are trying to do to guard those borders and those strategic points of crossing.

And I will let it go at that. I have a couple of other things I want to ask you, but I will send those to you. But I really want you to get me an answer that I can take back to Niagara Falls that is going to make some sense to them up there as to why Livingston County, a rural dairy county, which is quite beautiful, and we love it to pieces, why did they get overtime COPS grants, and Niagara Falls didn't?

And if it is a political issue, I cannot tell you how angry I am going to be. Thank you.

Mr. VERDERY. Well, I can hear your concerns. I will take them back and report back as promptly as we can.

Chairman COX. And we will leave the hearing record open so that we can have that answer expressed fully in the record. I want to thank all of our witnesses for bearing with us through several hours.

This was an extremely informative and constructive hearing. The hearing is adjourned.

[Whereupon, at 4 p.m., the committee was adjourned.]

MATERIALS SUBMITTED FOR THE RECORD

QUESTIONS FOR THE RECORD FOR MR. JOSEPH R. CARICO FROM THE HONORABLE CHRISTOPHER COX

Question: What happens if the application is denied before the expiration of the driver's license?

Answer: Virginia's new legal presence law provides that DMV is not to issue a driver's license or identification card to an applicant who is the subject of a notification from a federal, state or local federal government agency indicating that the individual is not lawfully present in the United States pursuant to § 46.2–328.1(c) of the Code of Virginia. In order for such an applicant to obtain a subsequent document, the individual must provide DMV with documentation that proves they are in the United States lawfully. As currently written, the law does not require DMV to obtain immigration application status updates for these DMV document bearers, but will require DMV to take action if the agency is notified by law enforcement that such an applicant is no longer lawfully present in the United States.

Question: Are DMV offices notified that they have someone out there who shouldn't have a driver's license?

Answer: In Virginia's new legal presence law, provision has been made for DMV to receive notice from local, state and federal agencies that a licensed driver or identification card holder is no longer lawfully present in the United States.

Question: How about when BCIS take more time than they expected, are states updated so that these people that deserve a driver's license are not driving around with expired licenses?

Answer: We are not aware of any notification system that may have been implemented by BCIS that would provide states with automatic updates concerning pending applications. Once the new law is implemented, we anticipate that individuals who have pending applications on file with BCIS and whose driver's license is about to expire will take measures to apply for a new driver's license. DMV is planning to use specialists to address such situations. The specialists will consider an applicant's situation and attempt to determine whether the applicant is eligible for another driver's license. It is likely that the determination of whether the applicant is eligible to receive a new driver's license will include an inquiry to BCIS.

QUESTIONS FOR THE RECORD TO THE HONORABLE STEWART VERDERY FROM THE HONORABLE LINCOLN DIAZ-BALART

Question: Currently, BCIS provides immigration applicants a receipt indicating that BCIS is processing their application and the estimated time it will take to approve or deny the application. States then issue a drivers license for that period of time, even though it usually takes more time for BCIS to process the applications because of their large application backlog. What happens if the application is denied before the expiration of the driver's license? Are DMV offices notified that they have someone out there who shouldn't have a driver's license? How about when BCIS take more time than they expected, are states updated so that these people that deserve a driver's license are not driving around with expired licenses.

Answer: State Departments of Motor Vehicles (DMVs) can participate in the Systematic Alien Verification for Entitlements (SAVE) Program in order to electronically obtain immigration status information when an individual applies for a driver's license or state-issued identification card. DHS/USCIS will verify the immigration status of the applicant, but will not make any recommendation to the state DMV whether to issue a driver's license or state-issued identification card.

The SAVE Program is responsible for administering DHS/USCIS programs involving customer access to the Alien Status Verification Index (ASVI) database. Access to ASVI enables federal, state, and local government agencies to obtain immigration status information needed to determine an applicant's eligibility for many public benefits. Several state DMVs participate in the SAVE Program. At the present time, California, Florida, New Jersey, New York, Virginia, and Wyoming have signed a Memorandum of Understanding to participate. In FY 2003 over 674,000 queries were performed by these states. Indiana and Colorado have also expressed interest in participating.

A personal computer with modem and software is used to access the information. In most cases, immigration status information will be provided electronically within seconds of the request. When the system cannot provide the immigration status immediately, the inquiring state DMV must enter additional information and electronically send the query to DHS. That query is transmitted to an immigration status verifier (ISV) for an additional verification check. The response to queries requiring additional verification is usually provided within 3 workdays. Federal, state, and local government agencies are charged a fee for queries conducted -- 24 cents for an initial query, and 24 cents for an ISV verification.

USCIS issues receipt notices when an application or petition is filed for immigration benefits. The receipt notice establishes that an application/petition was filed and usually indicates the estimated amount of time it will take to process that application. When the application is adjudicated, only the petitioner/applicant or their attorney is notified in writing of the decision. Recently USCIS began posting processing times on the Internet for all form types at all District Offices, Service Centers, and at the National Benefits Center. The dates are moving dates and indicate the receipt date of the work currently being adjudicated. You can find more about this on the USCIS website at www.uscis.gov.

QUESTIONS FOR THE RECORD TO THE HONORABLE STEWART VERDERY FROM THE HONORABLE LOUISE M. SLAUGHTER

Question: Moving beyond the current debate over the first responder grant system, would he agree that we need to create a method to identify and provide what cities, counties, and states need in order to be prepared to handle a terrorist attack?

Answer: The Department of Homeland Security firmly believes that it is essential to provide states and localities the support they need to enhance their security against terrorist attacks, and to provide them the resources to identify vulnerabilities and needs. To this end, the Department, through ODP, administered the State Homeland Security Assessment and Strategy Process (SHSAS). This process allowed states and local jurisdictions to update their needs and vulnerabilities assessment to reflect post-September 11, 2001, realities, as well as to identify progress on the priorities outlined their initial homeland security strategies, which were initially conducted in 1999. The SHSAS process allows states to make prudent and informed decisions on how best to allocate and distribute funds they receive from ODP and DHS to enhance their security.

In addition, ODP is continuing its efforts to develop preparedness standards and to establish clear methods for assessing State and local preparedness levels and progress. On December 17, 2003, the President issued "Homeland Security Presidential Directive (HSPD)–8." Through HSPD–8, the President tasked Secretary Ridge, in coordination with other Federal departments and State and local jurisdictions, to develop national preparedness goals, improve delivery of federal preparedness assistance to State and local jurisdictions, and strengthen the preparedness capabilities of Federal, State, territorial, tribal, and local governments.

Earlier this year, the Secretary delegated to ODP the lead for the implementation of HSPD–8. This designation by the Secretary is consistent with ODP's mission, as provided under the provisions of the Homeland Security Act, to be the primary federal agency responsible for the preparedness of the United States for acts of terrorism. HSPD–8 is consistent with the broader goals and objectives established in the President's National Strategy for Homeland Security issued in July, 2002, which discussed the creation of a fully-integrated national emergency response capability. Inherent to the successful implementation of HSPD–8 is the development of clear and measurable standards for State and local preparedness capabilities.

The standards that will result from HSPD–8 implementation build on an existing body of standards and guidelines developed by ODP and other Federal agencies to guide and inform State and local preparedness efforts. Since its inception ODP has worked with Federal agencies and State and local jurisdictions to develop and disseminate information to State and local agencies to assist them in making more in-

formed preparedness decisions, including capability assessments, preparedness planning and strategies, and choices relating to training, equipment, and exercises.

Question: As the Council on Foreign Relations Task Force recently stated, "The absence of a functioning methodology to determine national requirements for emergency preparedness constitutes a public policy crisis. Establishing national standards that define levels of preparedness is a critical first step toward determining the nature and extent of additional requirements and the human and financial resources needed to fulfill them." Does he agree with this assessment?

Answer: The Secretary firmly supports the need to establish national standards and preparedness levels. Through HSPD–8, the Department is developing of clear and measurable standards for State and local preparedness capabilities. This process will result in the development of national preparedness goals, and will improve delivery of federal preparedness assistance to State and local jurisdictions. The work completed under HSPD–8 will also strengthen the preparedness capabilities of Federal, State, territorial, tribal, and local governments.

The standards that will result from HSPD–8 implementation build on an existing body of standards and guidelines developed by ODP and other Federal agencies to guide and inform State and local preparedness efforts. Since its inception ODP has worked with Federal agencies and State and local jurisdictions to develop and disseminate information to State and local agencies to assist them in making more informed preparedness decisions, including capability assessments, preparedness planning and strategies, and choices relating to training, equipment, and exercises.

Question: What is DHS doing internally to develop such a criteria?

Answer: On December 17, 2003, the President issued "Homeland Security Presidential Directive (HSPD)–8." Through HSPD–8, the President tasked Secretary Ridge, in coordination with other Federal departments and State and local jurisdictions, to develop national preparedness goals, improve delivery of federal preparedness assistance to State and local jurisdictions, and strengthen the preparedness capabilities of Federal, State, territorial, tribal, and local governments.

Earlier this year, the Secretary delegated to ODP the lead for the implementation of HSPD–8. This designation by the Secretary is consistent with ODP's mission, as provided under the provisions of the Homeland Security Act, to be the primary federal agency responsible for the preparedness of the United States for acts of terrorism. HSPD–8 is consistent with the broader goals and objectives established in the President's National Strategy for Homeland Security issued in July, 2002, which discussed the creation of a fully-integrated national emergency response capability. Inherent to the successful implementation of HSPD–8 is the development of a national preparedness goal that will include clear and measurable standards for State and local preparedness capabilities.

The standards that will result from HSPD–8 implementation build on an existing body of standards and guidelines developed by ODP and other Federal agencies to guide and inform State and local preparedness efforts. Since its inception ODP has worked with Federal agencies and State and local jurisdictions to develop and disseminate information to State and local agencies to assist them in making more informed preparedness decisions, including capability assessments, preparedness planning and strategies, and choices relating to training, equipment, and exercises.

Question: Would he agree that such a risk criteria be the basis for first responder grant allocations?

Answer: The language in the President's Fiscal Year (FY) 2005 request for the Department of Homeland Security recognizes that factors other than a minimum formula and population should be considered in making overall funding allocations. The language further states that the Secretary should have the latitude to and discretion to make this determination based on a number of factors, including population concentrations, critical infrastructure, and other significant terrorism risk factors.

Terrorism and the threat of terrorist acts are not static, as is the current formula included in the USA PATRIOT Act. Instead, threats, risks, and vulnerabilities are fluid and can change based on a number of factors. The Department of Homeland Security should not be constrained by a formula and distribution method that does not change to meet current and future security needs. As you know, each state has submitted an updated homeland security strategy as a requirement of receiving and distributing FY 2004 Office for Domestic Preparedness grant funds. It is the Department's expectation that these strategies, and periodically updated strategies, will provide invaluable information to determine appropriate funding levels for all states—large and small, urban and rural.

The Administration and Congress share the goal of enhancing the nation's ability to deter, prevent, respond to, and recover from acts of terrorism. The Administration firmly supports the notion that security needs to be improved across the nation. The

Administration strongly supports a change in the USA PATRIOT Act formula so that we can apply more factors than just population to distributing and expending limited homeland security resources.

QUESTIONS FOR THE RECORD FOR MR. PAUL J. MCNULTY, UNITED STATES ATTORNEY FROM THE HONORABLE LINCOLN DIAZ-BALART

Question: Currently, BCIS provides immigration applicants a receipt indicating that BCIS is processing their application and the estimated time it will take to approve or deny the application. States then issue a drivers license for that period of time, even though it usually takes more time for BCIS to process the applications because of their large application backlog. What happens if the application is denied before the expiration of the driver's license? Are DMV offices notified that they have someone out there who shouldn't have a driver's license? How about when BCIS take more time than they expected, are states updated so that these people that deserve a driver's license are not driving around with expired licenses.

Answer: It is my understanding that the Department of Homeland Security's Bureau of Citizenship and Immigration Services ("BCIS") is required by law to provide an application receipt, I–797C, when an immigrant applicant submits an application to them. The I–797C indicates that the BCIS has received an application and that the application is being processed. The I–797C also provides an estimated time that will be required to process the application. It is also my understanding that BCIS does not issue this document for it to be used as a form of identification to assist the immigrant applicant in obtaining a valid driver's license from the state in which he or she lives. As I stated previously, this document simply acknowledges that BCIS is in receipt of an immigrant application and that it will be processed in the future.

State law determines whether a valid driver's license will be issued based on a presentation of an I–797C. I am told that some states, such as Congressman Diaz-Balart's home state of Florida, do in fact issue immigrant applicants valid driver's licenses based on the presentation of the I–797C. In the Commonwealth of Virginia, the I–797C is accepted as a secondary document in support of proof of identity.

In Virginia, an applicant for a driver's license is required to present two forms of identification, a primary document and a secondary document to the Department of Motor Vehicles ("DMV") in order to obtain a driver's license. If the applicant meets the additional proof of residency requirement, he is issued a valid Virginia license. This license is issued for an approximately five-year time period. It is not issued to correspond with the estimated time of adjudication of the immigrant application. Thus, the adjudication of the immigrant application does not have any affect on the validity of the Virginia license. If the immigrant application is denied after the license has been issued, that individual still has a valid license until it expires. It is my understanding that BCIS does not inform the DMV of the denial, nor does DMV inquire with BCIS to determine the status of the application. No communication exists between the BCIS and the DMV. In Virginia, the adjudication of the immigrant application does not affect the validity of the individual's license.

Finally, I want to compliment the Virginia legislature for its new legal presence law, which will be effective on January 1,2004. hi my judgment, this law is a step in the right direction towards ensuring the integrity of the documents produced and issued by the Virginia DMV. As I understand it, the legal presence law will require an individual applying for a driver's license or identification card for the first time to prove that he is either a United States citizen or is legally authorized to be in the United States.

QUESTION FOR THE RECORD FOR MR. JOHN PISTOLE FROM CONGRESSMAN LINCOLN DIAZ-BALART

Currently, BCIS provides immigration applicants a receipt indicating that BCIS is processing their application and the estimated time it will take to approve or deny the application. States then issue a drivers license for that period of time, even though it usually takes more time for BCIS to process the applications because of their large application backlog. What happens if the application is denied before the expiration of the driver's license? Are DMV offices notified that they have someone out there who shouldn't have a driver's license? How about when BCIS take more time than they expected, are states updated so that these people that deserve a driver's license are not driving around with expired licenses.

[No Response was received.]

QUESTION FOR THE RECORD FOR MR. RONALD D. MALFI FROM THE HONORABLE LINCOLN DIAZ-BALART

Currently, BCIS provides immigration applicants a receipt indicating that BCIS is processing their application and the estimated time it will take to approve or deny the application. States then issue a drivers license for that period of time, even though it usually takes more time for BCIS to process the applications because of their large application backlog. What happens if the application is denied before the expiration of the driver's license? Are DMV offices notified that they have someone out there who shouldn't have a driver's license? How about when BCIS take more time than they expected, are states updated so that these people that deserve a driver's license are not driving around with expired licenses.

[No Response was received.]

QUESTION FOR THE RECORD FOR MR. ROSCOE C. HOWARD, JR. FROM THE HONORABLE CHRISTOPHER COX

Currently, BCIS provides immigration applicants a receipt indicating that BCIS is processing their application and the estimated time it will take to approve or deny the application. States then issue a drivers license for that period of time, even though it usually takes more time for BCIS to process the applications because of their large application backlog. What happens if the application is denied before the expiration of the driver's license? Are DMV offices notified that they have someone out there who shouldn't have a driver's license? How about when BCIS take more time than they expected, are states updated so that these people that deserve a driver's license are not driving around with expired licenses.

[No Response was received.]

QUESTIONS FOR THE RECORD FOR MR. KEITH KISER FROM THE HONORABLE LINCOLN DIAZ-BALART

AAMVA submitted Representative Lincoln Diaz-Balart's questions to our membership through the Driver's Licensing Yahoo Group. We received 33 responses back, which are attached. AAMVA has summarized the answers to respond to the Committee's questions.

Question: 1. Does your jurisdiction tie the expiration date of the driver's license to immigration documents?

Answer: Approximately 15 states tie the expiration date of the driver's license to the expiration date of immigration documents.

Question: 2. Will your jurisdiction issue a driver's license for individuals possessing a receipt of application from the Bureau of Citizenship and Immigration Services (BCIS)?

Answer: A majority of motor vehicle agencies will not issue a driver's license to an individual possessing a receipt of application from BCIS. For those motor vehicle agencies that do accept a receipt, they usually require the individual to submit other documentation from the agency's list of approved documents.

Question: 3. What happens if the application submitted to BCIS is denied before the expiration of the driver's license issued?

Answer: MVA's usually do nothing if the BCIS application is denied before the expiration of the driver's license. A majority will allow the driver's license to expire. However, a few of the motor vehicle agencies cancel or revoke the driver's license.

Question: 4. Are you linked in any way to the BCIS with regard to the denial or approval of applicants? If yes, please indicate the manner in which you receive this information.

Answer: A majority of motor vehicle agencies are not linked electronically to BCIS so they have no way of knowing whether an application has been denied or approved. A few of the states are linked to BCIS SAVE system (e.g., Florida) but a majority attempt to call their local BCIS to obtain information for special situations.

States	Does your jurisdiction tie the expiration date of the driver's license to immigration documents?	Will your jurisdiction issue a driver's license for individuals possessing a receipt of application from the Bureau of Citizenship and Immigration Services (BCIS)?	What happens if the application submitted to BCIS is denied before the expiration of the driver's license issued?	Are you linked in any way to the BCIS with regard to the denial or approval of applicants? If yes, please indicate the manner in which you receive this information.
Alabama				
Alaska	Alaska does not tie the expiration of immigrant docs to the DL	NO	N/A	NO, but if any document is questionable we call and verify validity.
Arizona	YES.	YES. EXPIRATION DATE IS TIED TO THE RECEIPT.	LICENSE WILL NOT BE EXTENDED.	NO.
Arkansas	No.	No.	N/A.	No
California				
Colorado	YES	NOT JUST WITH THE RECEIPT	THE LICENSE WOULD REMAIN VALID UNTIL THE EXPIRATION DATE	NOT YET
Connecticut	No. Legislation was proposed during our last session to do so. It passed the Senate by a very narrow margin and never came to a vote in the House.	We require a receipt or Notice of Action for adjustment of status to legal permanent resident from applicants who hold a Bi or B2 visa because we do not issue a license or ID card to visitors or illegal aliens. If the applicant has a valid passport and an employment authorization card, we will issue as long as they provide the receipt indicating they have applied for the adjustment of status.	The license is valid until expiration.	We run a check through NLETS to the BCIS Law Enforcement Support Center using information from the identity documents presented and wait for a response.
Delaware	No	No, Delaware does not accept applications as proof of being legally in this Country.	No	No
District of Columbia				

States	Does your jurisdiction tie the expiration date of the driver's license to immigration documents?	Will your jurisdiction issue a driver's license for individuals possessing a receipt of application from the Bureau of Citizenship and Immigration Services (BCIS)?	What happens if the application submitted to BCIS is denied before the expiration of the driver's license issued?	Are you linked in any way to the BCIS with regard to the denial or approval of applicants? If yes, please indicate the manner in which you receive this information.
Florida	Yes. In most cases. If there is an expiration date on the document presented for non-immigrants, such as an Employment Authorization Card, 1–20, etc., then license expiration will coincide with that date. When documents are under process and hence no expiry date is available but the customer is in the country lawfully, all non-immigrants will be issued a license for not more than 2 years. All Permanent Residents (with a green card or an ADIT stamp on their passport/I–94) will be issued a normal duration license/ID card. The only expiration date not considered by us is the date on the 1–551/151, the Resident Alien Card or the ADIT stamp on the passport/I–94.	Yes.	First, they will have been issued a license as a non-immigrant. Hence they can only have it for 2 years. They have to produce evidence of lawful presence every time they need a service and this will lay them open to being rejected. Where we are not notified at all, the 2-year duration will be the determinant,	We are connected to the SAVE system both for individual queries and for batch verification. When the response to a secondary verification comes back unverified, then our procedures will prevent the continuance of the license. There are possibilities that some will get through the cracks and have validity for 2 years.
Georgia				
Guam				
Hawaii	No.	No.	Not applicable.	DMV calls the duty officer for verification whenever they suspect the applicant possesses illegal documents.
Idaho	Idaho no.	Idaho no.	Idaho N/A	Idaho no.

States	Does your jurisdiction tie the expiration date of the driver's license to immigration documents?	Will your jurisdiction issue a driver's license for individuals possessing a receipt of application from the Bureau of Citizenship and Immigration Services (BCIS)?	What happens if the application submitted to BCIS is denied before the expiration of the driver's license issued?	Are you linked in any way to the BCIS with regard to the denial or approval of applicants? If yes, please indicate the manner in which you receive this information.
Illinois	No	No. We will, however, accept identification from the Department of Justice indicating the applicant's refugee status (this document often has a photo and a metal grommet affixed to the document). We will accept this document for proof of date of birth in these cases. Regardless, the applicant must still provide a SSN card and a proof of residency document.	N/A	No
Indiana	No	Yes, but only with INS verification that legal status is pending.	Licensed revoked.	No direct electronic link . However, we can call if we need to.

States	Does your jurisdiction tie the expiration date of the driver's license to immigration documents?	Will your jurisdiction issue a driver's license for individuals possessing a receipt of application from the Bureau of Citizenship and Immigration Services (BCIS)?	What happens if the application submitted to BCIS is denied before the expiration of the driver's license issued?	Are you linked in any way to the BCIS with regard to the denial or approval of applicants? If yes, please indicate the manner in which you receive this information.
Iowa	Yes	Yes, providing the petition to adjust or amend status was made before the original status expired.	We limit the renewal to a term of 120 days (Iowa statute caps it at two years). If the petition is denied, we could cancel the license or ID if the denial became know to us. However, we do not track them. Since a ruling on a petition often takes a long time, we are under pressure from advocates of immigrants to issue for the period of time the ruling is pending. We seem to get mixed responses when we consult with federal immigration officials, Those in the investigation/enforcement side of things, say a person has no benefits when a petition is pending and if the original status is expired, we should not issue. Immigration officials on the benefits side of things, seem to suggest that since they are allowed to stay in the country unti the petition is ruled on, we should issue. We really have no clear direction.	No. However, we have used the federal immigration court system number and have checked via the A# for those persons who are scheduled to appear before an immigration judge. That number is 1–800–898–7180. We have also verified petitions and Notices of Action with the LIN receipt number via the 1–800–375–5283 number. Our agency's motor vehicle investigators have local contacts with BCIS, who are helpful also.
Kansas	No, except on non-resident CDL's (by Kansas statute).	No	N/A	The only link we have is direct contact with agents in the Kansas City and Wichita offices. We use these contacts for special situations regarding legitimacy of documents that are in applicant's possession.

States	Does your jurisdiction tie the expiration date of the driver's license to immigration documents?	Will your jurisdiction issue a driver's license for individuals possessing a receipt of application from the Bureau of Citizenship and Immigration Services (BCIS)?	What happens if the application submitted to BCIS is denied before the expiration of the driver's license issued?	Are you linked in any way to the BCIS with regard to the denial or approval of applicants? If yes, please indicate the manner in which you receive this information.
Kentucky	Yes	No. We will allow a one year license for individuals applying to extend or change their status provided they have an official notice of action from BCIS.	The current license remains valid until the end of the one year period. At that point the individual is not allowed to renew.	No
Louisiana	Louisiana is currently working on a Next Generation Motor Vehicle system that will address many issues. Currently, Louisiana does require proof of legal presence in order to issue a license or ID card. However, the current computer system still issues a 4 year license. This will not be the case with the NGMV system. The expiration date of the license credential will be tied in with the immigration documents. At this point, it is not.	Louisiana uses AAMVA list of identification documents. The applicant is required to submit proof of legal presence, not just application for legal presence.		No connectivity to the BCIS.
Maine	No	As secondary documentation only. Additional INS documents, or passport/visa and 1–94 required.	See #2	See #2
Maryland	No	Yes, it would have no bearing on their application. They would be required to be an Maryland resident, show proper identification and meet all other application requirements such as passing any required tests and paying fees.	Nothing	No
Massachusetts				
Michigan				

States	Does your jurisdiction tie the expiration date of the driver's license to immigration documents?	Will your jurisdiction issue a driver's license for individuals possessing a receipt of application from the Bureau of Citizenship and Immigration Services (BCIS)?	What happens if the application submitted to BCIS is denied before the expiration of the driver's license issued?	Are you linked in any way to the BCIS with regard to the denial or approval of applicants? If yes, please indicate the manner in which you receive this information.
Minnesota	Yes, if the applicant presents temporary legal presence documents, the date the documents expire is shown as a ''status check date'' on the driver's license or identification card.	Yes, if they are able to also submit documentation for our list of approved Primary and Secondary Documents, or they submit a variance request and through that request can provide adequate information to prove their identity and legal residency.	If the applicant submits a receipt with no Duration of Status or expiration date on it, the Status Check on the driver's license or Identification card would expire in 6 months and the cardholder's privileges would be cancelled. To prevent cancellation, the cardholder would need to present updated information to prove that BCIS had approved the application by submitting the document itself for review.	Minnesota has a contact that we call to find out approval or denial of applicants. That information is then noted as a memo on the application.
Mississippi				
Missouri	No, not at this time.	No, Missouri does not accept a receipt of application as acceptable proof of identity.	N/A	Not in our field offices. Our central office has a system in place for exception processing.
Montana				
Nebraska	No.	No,	N/A.	No.
Nevada	Effective January 1, 2004, we will tie the expiration dates of the immigration documents to both driver's licenses and identification cards.	We do not issue a license until the BCIS has approved the application	Not applicable	No
New Hampshire				
New Jersey				
New Mexico				

States	Does your jurisdiction tie the expiration date of the driver's license to immigration documents?	Will your jurisdiction issue a driver's license for individuals possessing a receipt of application from the Bureau of Citizenship and Immigration Services (BCIS)?	What happens if the application submitted to BCIS is denied before the expiration of the driver's license issued?	Are you linked in any way to the BCIS with regard to the denial or approval of applicants? If yes, please indicate the manner in which you receive this information.
New York	No. New York State has implemented a temporary visitor program which places in bold letters a legend on the face of the document indicating that the individuals legal status is temporary and also places the expiration date of their legal status in the United States on the document. Additionally, any further transaction processing is prohibited once the legal status has expired.	No. We require original valid INS documents that have been issued for at least a one-year stay with at least six months of legal status remaining.	N/A	We will shortly be commencing a pilot of the SAVE program to verify INS documents on line with the BCIS.
North Carolina	Not at this time. We would consider it if there was an easy (i.e. online) process for verifying information. But given the complexity of immigration documentation, we hesitate to attempt that at this time.	North Carolina does not require proof of legal presence for issuance of a DL or ID card. Any document issued by BCIS could be used as a form o identification to meet the state's requirements.	Not applicable, given that we don't require proof of legal presence.	No. Occasionally we may call them to verify documents presented to us, but it can be extremely difficult to get through to them (they have the same understaffing problem most DMVs have).
North Dakota	No	No	Not Applicable	No
Ohio	YES	YES	CANCEL THE LICENSE	NO

States	Does your jurisdiction tie the expiration date of the driver's license to immigration documents?	Will your jurisdiction issue a driver's license for individuals possessing a receipt of application from the Bureau of Citizenship and Immigration Services (BCIS)?	What happens if the application submitted to BCIS is denied before the expiration of the driver's license issued?	Are you linked in any way to the BCIS with regard to the denial or approval of applicants? If yes, please indicate the manner in which you receive this information.
Oklahoma	YES	THERE ARE TWO TYPES OF RECEIPTS WE ARE AWARE OF: ONE SIMPLY SHOWING PAYMENT RECEIVED AND ANOTHER HAS A EMPORARY 1–94 ON IT. WE DO NOT ACCEPT THE RECEIPT SHOWING ACKNOWLEDGMENT OF APPLICATION AND FEES. WE DO ACCEPT, HOWEVER, THE RECEIPT THAT CONTAINS THE 1–94. WERE TOLD THAT THE ONLY CASES WHERE THE 1–94 RECEIPTS ARE ISSUED IS WHEN THE BACKGROUND CHECK HAS BEEN COMPLETED AND THE OFFICIAL PERMANENT DOCUMENT IS ALL BUT ISSUED.	IT IS OUR UNDERSTANDING THAT SINCE WE ONLY ISSUE LICENSES BASED ON THE RECEIPT WITH 1–94 THAT THE DENIAL OF THE INDIVIDUAL WOULD BE EXTREMELY UNLIKELY AS THE BCIS SCREENING PROCESS HAS ALREADY BEEN COMPLETED.	OUR ONLY LINK WITH BCIS IS THROUGH A VERY GOOD DIALOGUE WITH BCIS OFFICIALS IN THIS STATE. AS YOU KNOW WE DO NOT HAVE ANY ELECTRONIC INTERFACE WITH BCIS AT THIS TIME TO IMMEDIATELY CHECK STATUS NOR RECEIVE CHANGES IN STATUS.
Oregon	No	Yes, it would have no bearing on their application. They would be required to be an Oregon resident, show proper identification and meet all other application requirements such as passing any required tests and paying fees.	Nothing	No
Pennsylvania				
Puerto Rico				
Rhode Island				
South Carolina				
South Dakota	Yes.	No	N/A	We do some verbal/phone verification of documents. We also access NLETS to verify INS documents.

States	Does your jurisdiction tie the expiration date of the driver's license to immigration documents?	Will your jurisdiction issue a driver's license for individuals possessing a receipt of application from the Bureau of Citizenship and Immigration Services (BCIS)?	What happens if the application submitted to BCIS is denied before the expiration of the driver's license issued?	Are you linked in any way to the BCIS with regard to the denial or approval of applicants? If yes, please indicate the manner in which you receive this information.
Tennessee				
Texas	No	Our rule requires that the applicant have valid BCIS documentation, If this application extends the validity period of those documents, it would be acceptable.	If the applicant is issued a DL/ID based on that document in conjunction with other acceptable documentation, the applicant would be allowed to keep the DLIID.	No
Utah	No	Yes, if they have other acceptable ID	N/A	No
Vermont	No	No	N/A	No, the exception is some phone contact to vertify documents.
Virgin Islands				
Virginia	Virginia will effective 1/1/04, the following responses apply after 1/1/04	No	N/A	Not in customer service centers. We are considering having SAVE acess for only a very few persons, just to assist in exceptional situations.
Washington				
West Virginia	Yes, effective July 1, 2003	Not currently	N/A	No
Wisconsin	No	Person must show one document that verifies name and date of birth (passport, U.S. or foreign birth certificate, 1–151 or 1551, 1–181, 1–94 Refugee/Parolee, etc.) and proof of ID which is a document with either a photo or signature.	Document remains valid for period of issuance.	No.
Wyoming				

○