Identity and Security:

Moving Beyond the 9/11 Staff Report on Identity Document Security

February 2007

By Janice L. Kephart

Former Counsel to the 9/11 Commission
President, 9/11 Security Solutions, LLC

911securitysolutions.com

Table of Contents

Identity Document Security:
Moving Beyond the 9/11 Staff Report on Identity Document Security

All but one of the 9/11 hijackers acquired some form of U.S. identification document, some by fraud. Acquisition of these forms of identifications would have assisted them in boarding commercial flights, renting cars, and other necessary activities.
Recommendation: Secure identification should begin in the United States. The federal government should set standards for … sources of identifications, such as driver licenses.
Recommendation: The President should direct the Department of Homeland Security to lead the effort to design a comprehensive screening system, addressing common problems and setting common standards with system wide goals in mind.

The 9/11 Commission Report, p. 390, 387
July 2004

Introduction

Securing our identities and our identity documents is just as relevant today as it should have been on September 10, 2001. Identity establishes who we are as individuals, and who we are not. The issue of identity—verifying it and authenticating the documents used to prove it— underlay all the 9/11 Commission recommendations on secure IDs and current identity security law. In fact, perhaps the single most effective measure the United States can accomplish to lay the necessary framework for sustainable national and economic security and public safety is to shore up identity document issuance. Identity documents must be secure in their content, in their physical features, and in their issuance process. Without identity security at the base of our identity document issuance processes, our nation remains at risk. The reasons remain sound. This paper sets out the policy backdrop for the legislation that creates minimum standards for state-issuance of identity documents known as REAL ID, the Act's content, and what is at risk if it fails.

Executive Summary

The driver license (DL) today is a multi-use identity document. In today's America, we establish a person's identity primarily through state-issued DLs or personal identification cards (IDs). While the DL still holds its primary value in establishing state residency, motor vehicle registration or the legal right to drive, it is now relied upon for federal and state activities such as obtaining a passport, entering the United States over a land border, boarding aircraft and entering state and federal facilities, as well as private sector needs such as opening a bank account or picking up entertainment tickets for a local show.

For criminals, terrorists and others who want to live in the United States for nefarious purposes or under false guise, a state-issued DL or ID is their ticket to acquiring legitimate cover for their illegitimate activities. Those who seek to take advantage of a loose ID issuance system where neither identity nor residency is actually verified can do so when the system is set up to turn a blind eye to illegitimate applicants for state-issued DLs and IDs. The 9/11 hijackers did, as did many others less known both before and since. These types of individuals will continue

to put our national and economic security and our public safety at risk until the system is fixed to weed out legitimate from illegitimate applicants.

Recognizing both the significant federal and state interests in securing identification issuance processes, the Congress passed the REAL ID Act in 2005. REAL ID sets out minimum standards for state-issued DL/ID identification verification and card security that States can opt out of at their own choosing. The law was passed in May 2005 in response to the 9/11 Commission's findings of fact regarding the 9/11 hijackers' acquisition of 17 DLs and 13 IDs and presentation of those IDs to airline personnel on the morning of 9/11, as well as the Commission's recommendation that the federal government assure that driver licenses and state-issued IDs meet minimum standards of verification and authenticity. REAL ID repealed prior law that missed some key points in the 9/11 Commission recommendations, including insisting that only legitimate residents obtain legal identity documents that authenticate that they are, in fact, U.S. residents.

States must comply with REAL ID by May 2008 if their legal residents are to be able to use their DL/IDs for entry into certain federal facilities. However, the federal government is not openly discussing their progress on REAL ID nor has there been a request for a line item for REAL ID in the President's budget; nor is Congress showing support for providing assessed start-up costs to be spread amongst the 50 states and the federal government. Regulations are not yet out for comment, let alone published. According to a study by the National Governors Association, National Conference of State Legislators, and the American Association of Motor Vehicles (AAMVA), the initial capital investment required is around $1 billion. With so little forward momentum to date, REAL ID implementation at this point looks uneven at best.

In 2005, $40 million was appropriated but to date only $3 million released, with a $3 million grant awarded to New Hampshire that is to date still untouched. While some States are quickly coming into full compliance quietly, others are noisily objecting. The result is that the policy basis for REAL ID is being lost in the noise of issues that can readily be resolved. However, until regulations are available for comment and until an assessment and allocation of necessary 'bricks and mortar' start-up funding is in place, the REAL ID Act implementation is on hold and with that, all the vulnerabilities that REAL ID addresses remain in place as well. If laws regarding identity document security are taken seriously, our nation will be on a path to differentiate terrorists, criminals, and others from private citizens whose real life activities deserve real protection.

Section 1. 9/11 Commission Findings of Fact

The recommendations regarding secure identifications in the *9/11 Final Report* derive from the events laid out in the staff monograph *9/11 and Terrorist Travel* as investigated by the 9/11 Commission 'border team' and summarized in the *9/11 Final Report*. After 18 months of intense investigation, the border team found that the hijackers had not only engaged in flying lessons and terrorist financing operations, but in travel operations as well. Key to the hijackers' success was the ability to appear assimilated into the United States for the purpose of renting cars, obtaining living quarters, opening bank accounts, and of course, eventually boarding aircraft on the morning of 9/11. State-issued DLs and IDs were a one-stop shop for the hijackers' assimilation and movement within the United States. As I stated before the U.S. Senate Judiciary Committee on March 14, 2005: "The hijackers' acquisition of driver licenses and identification cards was clearly part of the hijackers' overall travel strategy."

1.1 Fraud and Misuse of State-Issued DLs and IDs by the 9/11 Hijackers[1]

The 9/11 hijackers engaged in a travel operation that included fraudulently obtaining 17 driver licenses in Arizona (1), California (2), Florida (14, four of which were duplicates), and 13 state-issued identifications from Florida (5), Maryland (1) and Virginia (7). All seven in Virginia were attained fraudulently and three of those hijackers presented those same IDs on the morning of 9/11 at Dulles ticket counters. We know six hijackers total presented state-issued IDs on the morning of 9/11, per recollection of airline personnel. We could surmise but will never know if others did as well.

Only one hijacker failed to apply for a state-issued ID. This same hijacker knew he had overstayed his immigration status and even tried to travel to the Bahamas to get an extended length of stay, but was denied entry because he did not have a visa. Our investigation led us to believe that the hijackers thought that DLs and IDs were linked to legitimate status in the United States, and were concerned that if this hijacker was found out to be illegally in the United States, the entire operation might unravel. Rather than risk that, it was decided that he would present his passport to airline personnel on the morning of 9/11. We know that he did.

The pilot who flew into the Pentagon, Hani Hanjour, had ID cards from Florida, Maryland and an Arizona DL. Despite his numerous state-issued IDs, Hanjour took the lead in helping himself and five of his fellow hijackers fraudulently obtain Virginia IDs on a scam that began on August 1, 2001. The next day, he became the only hijacker to not obtain the state-issued ID he sought, but it took him failing a Virginia DL test to actually not attain the state-issued ID.

1.2 The Virginia License Scams[2]

Three Salvadoran immigrants living in Virginia, two illegally and one as a lawful permanent resident, were found guilty of helping four 9/11 operatives use fraudulent documentation to obtain Virginia IDs. Two were convicted of helping Ahmed al Ghamdi and Abdul Aziz al Omari obtain fraudulent residency certificates on August 2, 2001. Another was convicted of providing false residency information on behalf of Hanjour and Mihdhar after being solicited by the two hijackers at a 7-Eleven in Falls Church, Virginia. For a fee, the Salvadoran falsely certified his old Virginia address as the residence of the hijackers. These residency certificates were then used to support their applications for Virginia identification cards issued by the Department of Motor Vehicles on August 1 and 2, 2001, respectively. The Salvadoran's address was also recycled by Moqed and Salem al Hazmi to use on their Virginia IDs issued on August 2, 2001. Jarrah followed suit on August 29, using a fictitious residency address and a certification of that address by Hanjour, who again used the address provided to him on August 1, 2001 to acquire his Virginia ID. One of the men charged in these cases recognized four of these hijackers as having been together at the Arlington, Virginia, DMV on August 2, 2001. In

[1] *See* 9/11 and Terrorist Travel: A Staff Report of the National Commission on Terrorist Attacks Upon the United States (Franklin, Tenn.: Hillsboro Press, 2004) at p. 44 for the table 'Identification Documents of the 9/11 Hijackers'. See the chapter 'The September 11 Travel Operation: A Chronology' for details of ID acquisition in the months preceding 9/11. To be clear, the page numbers for '9/11 and Terrorist Travel' that appear in this paper correspond to the book version of the monograph that I edited and corrected for publication, not the Web version. It is available in book form at http://providence-publishing.com/Merchant2/merchant.mvc?Screen=PROD&Store_Code=PP&Product_Code=9ATT&Category_Code=FTANR.*9/11 and Terrorist Travel*.
[2] *9/11 and Terrorist Travel*, p. 39. Textbox taken from report as originally written by Janice Kephart.

all, the five hijackers based their Virginia IDs on the residency information of one bribed Salvadoran.

1.3 Operational Command Mohamed Atta and Pennsylvania Pilot Ziad Jarrah

Four of the five 9/11 hijackers were stopped for speeding. However, the case of operational command and American Airlines Flight 11 pilot Mohamed Atta and United Airlines Flight 93 pilot Ziad Jarrah highlights how interwoven state-issued DLs and immigration status were to the hijackers' travel operation.

On September 9, 2001, Ziad Jarrah was stopped for speeding on I-95N at 90 miles an hour. Jarrah presented the state trooper with a Florida DL initially obtained on May 2, 2001. Also on May 2, Marwan al Shehhi, United Airlines Flight 175 pilot, re-entered the United States at Miami and acquired a six-month tourist length of stay. Al Shehhi already had obtained his Florida DL in April 2001, although he would acquire a duplicate in June 2001.

On the morning of May 2 prior to obtaining Jarrah's DL, Atta and, we believe, Jarrah were attempting to extend Jarrah's length of stay to September 2001 at the Miami Immigration Benefits office. Jarrah needed to solidify his U.S. assimilation. But they were unsuccessful. However, for Jarrah, while the length of stay extension would have been helpful, it was the DL he really needed. Not getting the extension of stay meant Jarrah would have to leave the United States again in July and re-enter to assure legal immigration status for the September operation, but not having a DL affected his ability to drive, open bank accounts and attain new residency. He and Atta both got their DLs (the only DL Atta would attain), but perhaps in a mix-up about where Jarrah would be flying from—Virginia or elsewhere—he would hastily acquire a Virginia ID card on August 29, 2001 as well. He did so by recycling pilot Hani Hanjour's false residency application of August 1, 2001.

Eventually Jarrah did have to leave in July, but when he did so, despite his illegal status, he was readmitted and given a length of stay through September 2001. Extending immigration status through September and obtaining a U.S. issued DL were thus two key steps in assuring ease of movement within the country under the radar of U.S. law enforcement.

What is more interesting about Jarrah's September 9 speeding ticket is that we do not know which DL he presented to the law enforcement officer who pulled him over. He had obtained a duplicate Florida DL on May 24, 2001. If Jarrah had been limited to one active DL, any prior driving citations may have been accessed and Jarrah been asked more questions. In addition, although Jarrah had illegally entered the U.S. at least five times, his immigration status was unavailable to state police. Instead, he slipped away with a $270 ticket. That ticket was found in the glove compartment of the car left at Newark Airport two days later when Jarrah boarded United Airlines Flight 93.

1.4 Use of State-Issued IDs on 9/11

At airline ticket counters on the morning of 9/11, airline personnel recalled that six hijackers used U.S. ID documents acquired in the previous months, three of which were fraudulently obtained in northern Virginia and used at Dulles during check-in. FAA regulations required that airline screeners view a government-issued identification as part of airline screening procedures. These IDs enabled the hijackers to avoid having to show screeners their Saudi,

Lebanese, and UAE passports to gain access to the planes. Airline personnel told us that the Virginia IDs did just that. In some instances, showing these passports on a domestic flight could have possibly triggered greater scrutiny, including at checkpoints where their knives and pepper spray could have been detected.
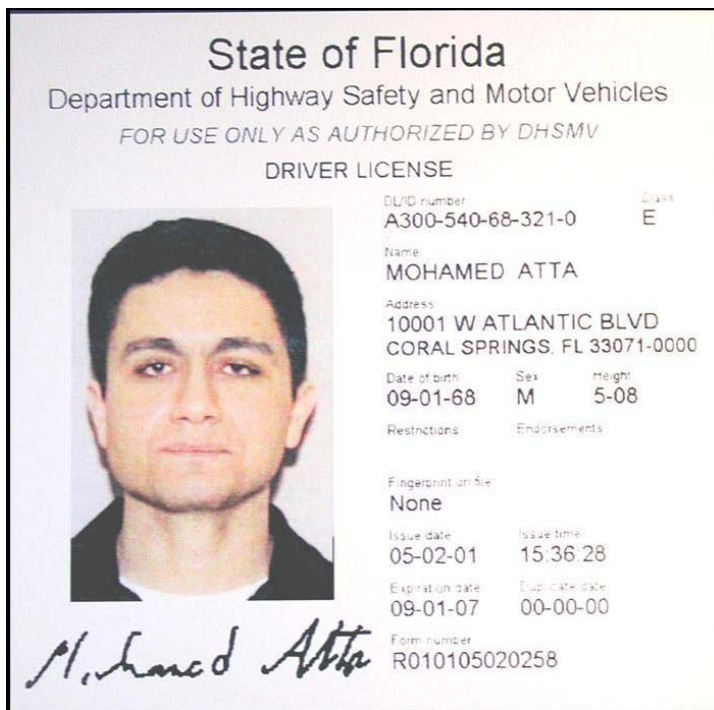
Copy of Mohamed Atta's Florida DL. Several other hijackers obtained Florida DLs including Hani Hanjour, Marwan al Shehhi, Nawaf al Hazmi, Ziad Jarrah, Waleed al Shehri, Hamza al Ghamdi, Ahmed al Nami, Ahmed al Haznawi, Saeed al Ghamdi, Mohand al Shehri, and Fayaz Banihammad.[3]

Section 2. 9/11 Final Report Recommendations

While on the Commission, we were only able to attain only information on exactly what means were used to acquire state-issued IDs in Virginia, and thus did not know if there were other instances of fraudulently obtained IDs. Certainly, in Virginia, fake residency certificates were recycled so that a total of seven hijackers were able to attain Virginia IDs, six of them on August 1 and 2, 2001 and one on August 29, 2001. Nor could we ascertain the strategy for obtaining the DLs.

However, what we could conclude was that acquiring DLs and IDs was part of an overall travel strategy whereby fraud was an essential aspect of each element of travel: using fraudulently altered passports, obtaining visas through fraud, obtaining entry through fraud, and obtaining immigration benefits through fraud. We think the hijackers obtained the state-issued IDs to help them stage their operation inside the United States, as these IDs allowed them to move freely around the country to meet, plan, and case targets, open bank accounts, rent cars, take flying lessons, and ultimately, board the airplanes on 9/11. We also knew that if the hijackers had been required to present birth certificates or residency applications subject to verification, they likely would have been unable to acquire the IDs.

---

[3] 9/11 and Terrorist Travel, p. A-18.

Our recommendation was therefore based on the premise that if foreign born persons with little or no right to be present in the United States can easily obtain state-issued IDs with little or no verification of their identity or travel status--federal or state--and assimilate into the United States, it will be easier for them to travel, case, meet, plan and carry out terrorist attacks inside the United States. Since state-issued IDs fill many of the assimilation needs of persons within the United States, we should take reasonable precautions to protect against their misuse. Creating minimum standards to secure IDs' content, their physical features, and their issuance process thus made common sense. Without setting a foundation for identity security, the system is perpetually at risk of being taken advantage of for a multitude of bad purposes, including terrorist activity.

2.1 Final Report Recommendation, July 2004

The *9/11 Final Report* provided six pages of findings of facts and recommendations on terrorist travel. Underlying these recommendations on terrorist travel intelligence, information-sharing, and screening was a clear recognition that these recommendations lose much of their value when law enforcement and intelligence at all levels cannot verify identity or authenticate identity documents. Thus, the following language in the report:

> All but one of the 9/11 hijackers acquired some form of U.S. identification document, some by fraud. Acquisition of these forms of identifications would have assisted them in boarding commercial flights, renting cars, and other necessary activities. *Recommendation*: Secure identification should begin in the United States. The federal government should set standards for birth certificates and sources of identification, such as driver licenses. Fraud in identification documents is no longer just a problem of theft. At many entry points to vulnerable facilities, including gates for boarding aircraft, sources of identification are the last opportunity to ensure people are who they say they are and to check whether they are terrorists.[4]

Also important to the border recommendations was the understanding that each time a person passes through a checkpoint provides another opportunity for a screening to "establish that people are who they say they are and are seeking access for their stated purpose, to intercept identifiable suspects, and to take effective action."[5] The report specifically mentions that one such checkpoint is when a foreign person is "inside the country, [for] they may seek another form of identification and try to enter a government or private facility."[6] The report continues:

> The job of protection is shared among these many defined checkpoints. By taking advantage of them all, we need not depend on any one point in the system to do the whole job. The challenge is to see the common problem across agencies and functions and develop a conceptual framework--an architecture--for an effective screening.[7]

---

[4] 9/11 Final Report, p. 390.
[5] Ibid. at p. 385.
[6] Ibid.
[7] Ibid. at p. 386.

2.2 Final Report on 9/11 Commission Recommendations, December 2005

In December 2005, a year and a half after the Commission was statutorily closed, and soon after the passage of the Intelligence Reform Act of 2005, the 9/11 Commissioners gathered one last time to issue a final report card on the implementation of their recommendations. The 9/11 Commissioners gave the government a B- for its work in standardizing and securing identifications, stating: "The REAL ID Act has established by statute standards for state-issued IDs acceptable for federal purposes, though states' compliance needs to be closely monitored."

Section 3. Other Terrorist Use of State-Issued IDs[8]

The 9/11 hijackers were not alone in using identity document fraud to assimilate into the United States. In a study I published in September 2005, *Moving Beyond the 9/11 Staff Report on Terrorist Travel,* other terrorists who had abused state-issued ID systems were discussed in detail. The report covered 94 terrorists (most of them indicted or convicted) who operated in the United States between the early 1990s and 2004, including the 9/11 hijackers. One of the findings of fact was that "seven terrorists were indicted for acquiring or using various forms of fake identification, including driver's licenses, birth certificates, Social Security cards, and immigration arrival records."[9] Some of these individuals were primarily terrorist supporters who were purveyors of illegitimate IDs, while others obtained legitimate IDs for terrorist activities.

One terror supporter who helped facilitate illegal entry and fraudulent acquisition of IDs was Muhammad Khalil, a self-proclaimed imam and basement mosque operator in Brooklyn. In September 2004 he was convicted on all counts for a variety of immigration and document fraud scams that included forging DLs, fraudulently obtaining legitimate Social Security cards, and sponsoring more than 200 applications for aliens seeking to obtain immigrant and nonimmigrant religious worker visas through the INS's religious worker program. He associated himself with al Qaeda, Osama bin Laden and Taliban leader Mullah Mohammed Omar. Khalil urged Muslims living in the United States to arm, and stated, "Hopefully, another attack in the United States will come shortly."[10]

Convicted terrorists also have abused the DL system. Take for example Mir Aimal Kansi, who killed two people outside CIA headquarters on January 25, 1993. He was able to case Washington D.C. and gain access to the CIA for the shootings under the guise of working as a courier. To become a courier he had to obtain a Virginia DL. He did so, despite being an illegal overstay and having fraudulently applied for both political asylum and amnesty under a 1986 law.[11] Again, there was no system in place that insisted on legal presence in the United States in order to attain a state-issued ID.

---

[8] Upon investigating current identity scams that could threaten our national security or public safety, I was shown fraudulently produced DLs, IDs and general aviation all-access IDs from a package intercepted by law enforcement in the summer of 2006. The IDs were of high quality and required a forensic determination as to whether they were counterfeit or not.
[9] Janice Kephart. *Immigration Benefits and Terrorism: Moving Beyond the 9/11 Staff Report on Terrorist Travel,* Center for Immigration Studies, Sept. 2005, p. 1.
[10] Ibid. at p. 29.
[11] Ibid. at p. 32.

Other terrorists have simply taken advantage of the ease in acquiring a legitimate state-issued DL, at times acquiring multiple DLs. In 2004, one terrorist with a pending terrorist-related prosecution still held a valid hazardous materials transport DL. This same terrorist had also held a commercial license to operate a school bus. Another held hazardous materials transport DLs from three different U.S. states. Two others worked with these terrorists as cab drivers in Boston. All four were associated with the Jordanian Millennium Plot to blow up American tourist attractions. Two of these terrorists were naturalized U.S. citizens.[12]

Another of the Millennium conspiracy associates, Nabil Al Marabh, was caught on June 27, 2001 trying to illegally enter the U.S. in the back of a tractor-trailer near Niagara Falls. He told authorities he had regularly traveled illegally between Canada and the United States. He had also received five DLs over 13 months from Massachusetts, Illinois, Ontario and Florida as well as a commercial DL and a permit to haul hazardous materials, including explosives and caustic chemicals. Al Marabh had stayed at a terrorist guesthouse in Pakistan known as the House of Martyrs, engaged in weapons training in Afghanistan, and worked for the Muslim World League—then an important source of al Qaeda's funds—in the early 1990s. Jordanian Millennium co-conspirators told authorities that Al Marabh was an al Qaeda operative. He was arrested after stabbing a man and had thousands of dollars worth of cash and amber jewels in his possession upon arrest.[13]

Section 4. Organized Criminal Enterprises and other Public Safety Concerns

Due to the increasing surge of identity theft and criminal busts of a variety of DL and ID scams, in March 2006 DHS Assistant Secretary Julie Myers created Document and Benefit Fraud Task Forces (DBFTF) within the Immigration and Customs Enforcement (ICE) agency.[14] The DBFTF mission statement makes clear that 'breeder' documents used to verify identities for the purpose of attaining state and federal-issued IDs are subject to significant

---

[12] "Before the 9/11 attacks, the FBI identified Mohammad Kamal Elzahabi as a suspected terrorist. Yet in early 2002, Elzahabi received a commercial driver's license to operate a school bus and transport hazardous materials. According to the Minnesota Department of Public Safety's Division of Driver Vehicle and Licensing, the FBI 'ran his name through a database and cleared him.' In June 2004, Elzahabi's license for transporting toxic materials was still valid, though his school bus driver's license had been canceled in February for reasons unknown. From 1997 to 1998 Elzahabi lived in Boston, working as a cabdriver. There he associated with Raed Hijazi, whom he aided in obtaining a Massachusetts driver's license in 1997. Raed Hijazi (born in California to Palestinian parents and later radicalized) was later convicted in Jordan for masterminding the failed Millennium bombing plot that had targeted American and Israeli tourists in that country. While in Boston, he lived with Bassam Kanj, who had married an American in 1988 and was later naturalized.146 Kanj helped Hijazi lease a taxi that officials believe was used to fund the Jordan plan. Also working with these taxi drivers was Nabil Al-Marabh, discussed in the illegal entry section below. Kephart, *Immigration and Terrorism,* p. 24-25.

[13] Janice Kephart, 9/11 Security Solutions, testimony before the U.S. Senate Judiciary Subcommittee on Immigration, Border Security and Citizenship and U.S. Senate Judiciary Subcommittee on Terrorism, Technology, and Homeland Security, *Border Security and Enforcement: The 9/11 Commission Staff Report on Training for Border Inspectors, Document Integrity, and Defects in the U.S. Visa Program,* March 14, 2005, p. 8-9.

[14] The Document and Benefit Task Forces are modeled on the multi-agency task force launched by the U.S. Attorney for the Eastern District of Virginia, Paul McNulty, who created the unit after conducting the prosecutions of individuals who provided false information and false documentation to 9/11 hijackers who obtained Virginia personal IDs. McNulty's model pulled the expertise of law enforcement involved in immigration and document related fraud and prosecutions resulting in some of the largest document and benefit fraud investigations in the nation have been prosecuted.

fraud, undermining security of the state-issued DL/ID systems. Currently there are 11 task forces, all in major metropolitan areas.[15] The DBFTF mission statement reads:

> Document and Benefit Fraud Task Forces Immigration fraud poses a severe threat to national security and public safety because it creates a vulnerability that may enable terrorists, criminals and illegal aliens to gain entry to and remain in the United States. … Individuals and criminal enterprises often use fraudulent documents to obtain drivers' licenses and social security cards. Traffickers and alien smugglers use these documents to facilitate movement into and within the United States and they are also used to shield illegal aliens from detection within our society. Fraudulent documents may be used to obtain financial benefits and entitlements intended for US citizens or lawful permanent residents and to obtain unauthorized employment.[16] The criminal investigations and prosecutions described below are in part accomplishments of these task forces.[17]

4.1 Castorena Family Organization

Beginning in the late 1980s and continuing until 2006, the Castorena family organization produced millions of high quality counterfeit fraudulent IDs including resident alien cards, social security cards, DLs, proof of vehicle insurance cards, temporary vehicle registration documents, and a host of other documents. American Express alone lost over $2 million just in Los Angeles due to the Castorena-produced fake IDs. The organization's leader worked out of Mexico, and money and documents flew across the southwest border and into all 50 states, with document-producing facilities and documents produced in most major U.S. cities. The Castorenas had more than 100 cell 'supervisors' with 10 to 20 'employees' in each cell. To date, agents have seized 20 document manufacturing laboratories and tens of thousands of

---

[15] To date, these Document and Benefit Fraud Task Forces have been initiated in 11 ICE Offices of the Special Agent in Charge to include Atlanta, Boston, Dallas, Denver, Detroit, Los Angeles, Newark, New York, Philadelphia, St. Paul and Washington, D.C., and each has works in tandem with their local U.S. Attorney's Office. Plans are underway for expansion.

[16] ICE Press Release. *Document and Benefit Fraud Investigations, Document and Benefit Fraud Task Forces,* Dec. 2006.
http://209.85.165.104/search?q=cache:qFcrV7vmliQJ:www.ice.gov/pi/news/factsheets/dbf061211.htm+document
+and+benefit+fraud+investigations+ICE&hl=en&gl=us&ct=clnk&cd=1&client=firefox-a

[17] ICE email to Janice Kephart, Feb. 17, 2007.

DBFTF Activity Since Inception (April 4, 2006)

	Cases Initiated	**Cases Closed**	**Search Warrants**	**Indictments**	**Criminal Arrests**	**Convictions**	**Seizures**
Atlanta	41	32	3	14	34	8	12
Boston	54	28	3	30	32	20	64
Dallas	89	19	16	71	68	6	244
Denver	16	1	4	0	20	0	12
Detroit	20	9	10	13	17	12	46
Los Angeles	77	49	18	28	53	51	23
New York	9	3	0	31	31	9	7
Newark	4	1	0	0	3	1	12
Philadelphia	42	19	6	26	25	13	21
St. Paul	81	22	14	52	64	30	61
Washington	17	4	2	13	33	28	28
Totals:	450	187	76	278	380	178	530

blank counterfeit identity documents, one silk screen press, 21 silk screen printing negatives/templates, 21 computers, 9 handguns and more than $100,000 in U.S. currency.[18]

In Denver alone, 20 computerized labs were seized and 50 persons were prosecuted and dozens of others deported to Mexico, Columbia, and El Salvador. Schedules were kept of vendor locations for marketing the counterfeit documents. City franchises were expensive to 'rent,' sometimes costing up to $15,000 per month, with money funneled to Mexico and elsewhere.[19] They competed with a rival document manufacturing organization, Los Acapulcos.[20]

Without minimum standards for ID physical security features nor a way for law enforcement to quickly and easily verify the legitimacy of the IDs, not to mention the private sector's inability to determine a fake from a legitimate ID, this organization operated unimpeded for nearly two decades before the federal government was able to shut it down. If tighter issuance standards had been in effect, the value of such fakes to potential customers would have been reduced while the organized criminals producing the fakes would have been at higher risk of getting caught.

4.2 Michigan Driver License Fraud Ring

From June 2003 to June 2004 two Brazilian citizens, one with a green card, conducted a DL fraud ring whereby they helped illegal aliens attain Michigan DLs. Michigan was chosen because it did not require proof of lawful status in the United States, a social security card, or actual residency in Michigan. The conspirators pled guilty to multiple counts of trafficking in fraudulent documents, alien smuggling and transporting illegal aliens to Michigan from the East Coast for the purpose of attaining DLs. The ring required production of 'breeder' documents in order to establish identity, and produced counterfeit foreign identity documents for this purpose. The conspirators then physically transported their clients into Michigan to complete applications, assist during the application process, provide false residency addresses in Eastern Michigan, and establish a mailbox where state-issued DLs were picked up. Eventually, their business expanded to include the smuggling of aliens into the U.S. from South American countries and immediately assimilated into the United States with fraudulently obtained state-issued DLs.[21]

With no requirement of lawful status, a social security card, or actual residency in Michigan, legitimate DLs were easily obtained for illegitimate purposes. And even if actual residency had been required under Michigan law, without a requirement for verification of residency, verification of other 'breeder' documents or a digital photo record to keep track of applicants, Michigan was an easy target for those seeking to take advantage of a weak state-issuance system.

---

[18] Michael Everitt, Unit Chief ICE Forensic Document Laboratory, DHS. Testimony before Senate Finance Committee, *Border Insecurity, Take Two: Fake IDs Foil The First Line of Defense.* August 2, 2006.
[19] Ibid.
[20] ICE email to Janice Kephart, Feb. 17, 2007.
[21] DOJ Press Release, 'Members of Driver's License Fraud Ring Please Guilty; Transported individuals to Michigan for Driver's Licenses.'

4.3 New Jersey and Pennsylvania Driver License Fraud Ring

In September 2005, eight people, including Ronald Henry, a former police officer working for the Pennsylvania Department of Transportation, were arrested for issuing hundreds of Pennsylvania DLs and commercial DLs to illegal aliens using 'breeder' documents—in this case, legitimate birth certificates from Puerto Rico—to pose as U.S. citizens. Altagarcia 'Grace' Rosario, with fellow conspirators, would provide these 'breeder' documents to Henry, who would use them to fulfill Pennsylvania identity requirements for DLs but then would falsify records indicating that DL testing had been passed and the individuals were entitled to a license.[22]

If Henry had been subjected to a background check and security clearance process, he may or may not have been unable to retain employment at the Pennsylvania DMV considering his prior employment as a police officer. However, a simple requirement that DMV employees be required to verify birth records electronically would have discouraged Rosario from attempting to use false 'breeder' documents to obtain the DLs or at least stopped the fraud early in its inception.

4.4 Identity Theft in the Swift Worksite Enforcement Case

The well-publicized Swift worksite enforcement case included identity theft of genuine birth certificates, DLs, state-issued ID cards, Social Security cards and other forms of IDs. These figures emerged when ICE submitted over 4,500 suspect employee names to the Federal Trade Commission Bureau of Consumer Protection's Identity Theft Database to determine if the true holders of these identities had reported identity theft either by phone or by internet. This database alone produced 326 matches and identified the perpetrators of an estimated $4 million in losses to the victims and their creditors.[23]

In the larger context of identity theft in general, in May 2006 the President created an Identity Theft Task Force that includes 17 government agencies and departments. In September 2006, the Task Force issued its first set of recommendations. Key among them was one calling on government agencies to work harder to protect personal data with best practices and create 'more reliable methods of authenticating the identities of individuals.'[24]

The Federal Trade Commission reported that between January 1 and December 31, 2005, there were about 4,600 reported cases of DL identity theft.[25] A sample study by a consumer nonprofit in 2004 noted that DL-related identity theft was a significant portion of non-banking

---

[22] http://www.ice.gov/pi/news/newsreleases/articles/050927newark.htm. Similar cases have come out of Florida (involving over 100 persons five of whom were DMV employees and over 2,000 documents) and Maryland (3 persons one of whom was still a DMV employee and over 100 state-issued IDs). http://www.ice.gov/pi/news/newsreleases/articles/050623washington.htm.

[23] ICE email to Janice Kephart, Feb. 17, 2007.

[24] http://www.ftc.gov/os/2006/09/060916interimrecommend.pdf

[25] This number is derived from tables 4 and 5, Identity Theft Victim Complaint Data, Federal Trade Commission, Jan. 1-Dec. 31, 2005. http://www.consumer.gov/idtheft/pdf/clearinghouse_2005.pdf. This data is the most current data available from the FTC.

identity theft, with 30 percent of victims suffering from having a counterfeit DL obtained using their identity information while 23 percent reported a state-issued DL obtained.[26]

Section 5. Essential Elements of Identity Security

Terrorists and criminals will continue to abuse state-issued identity systems until such systems are embedded with essential elements of security. This section reviews those elements in detail, providing a multi-tiered security approach that is more likely to reduce the value of fraudulent DLs and IDs in the black market and make those abusing the system more vulnerable to law enforcement action. None of these elements will stop fraud and abuse alone. However, each element, if insecure, permits a weakness that will continue to be taken advantage of if not strengthened.

5.1 Identity Information

A robust combination of identity information on a DL or ID is fundamental to assure accurate identification. Any one data field is insufficient without the others, and each provides an essential type of information necessary for a state to make an issuance decision on an applicant, and then secure that identification as unique. This identity information includes:

- o   The person's full legal name;
- o   The person's date of birth;
- o   The person's gender;
- o   The person's driver's license or identification card number;
- o   A digital photograph of the person;
- o   The person's address of principle residence;
- o   The person's signature.

By shifting to a multi-layered common data requirement, many of the problems that currently plague name-based issuance systems can be resolved. A full name will eliminate the problems that accrue when, for example, variances in names currently permitted on DLs and IDs in some states make it impossible to crosscheck whether that applicant holds other DLs or IDs or has a prior driver history. Simply requiring a full name increases the likelihood of an accurate match. The 9/11 hijackers, for example, had name variances in their DLs/IDs from those listed in their passport. A cross-state check with name variants would not have yielded information that the hijackers held other state-issued DLs/IDs. An insistence that full names be used may have.

Nearly all states do require that principal residence be verified. However, many states do not require verification of principal residence information be provided by the applicant. Such was a weakness in Virginia when the hijackers applied for the ID cards in August 2001, and a continuing problem in Michigan that alien smugglers benefited from. The residency requirement is one that deadbeat dads often avoid so as to hide their current location to avoid the federal law requirement of paying child support.

---

[26]Identity Theft: The Aftermath 2004, Identity Theft Resource Center (ITRC). Of note, the study found that hours spent by victims to recover from an identity theft was an average of 330 hours with a range of 3 hours to 5,840 hours, p.2. Forty percent of victims reported their individual losses greater than $15,000 with a $7,500 increase of $41,717 to $49,254 from 2003 to 2004. p.3. http://www.idtheftcenter.org/aftermath2004.pdf

A date of birth is another means to assure accurate checks and less delay in DL/ID issuance as well as watchlists issues that can arise at airports. Gender delineation and traceable numbers for the DLs/IDs (including those issued temporarily) are obvious support to verifying identity and assuring that counterfeit DLs/IDs are more quickly identified. This also enhances law enforcement officers at all levels to verify individual identity information when presented with state-issued DLs and IDs while protecting legitimate U.S. residents from economic and other crimes.

Digital photographs are essential to verifying identities. Without a biometric, a name-based only system will result in misidentifications, inconvenience, and will do little against counterfeiting. In 2005, more than 20 States were still using paper photos glued into license forms. This type of photo is easily manipulated and until passports were upgraded, it was the backbone of passport and other ID manipulation. All the counterfeiter had to do was break the plastic seal on the document and replace it with a photo of someone who has now 'stolen' the identity of the legitimate identity document holder. A digital photo protects true identities and helps root out fakes. Digitizing and maintaining photos of all DL/ID applicants so that fakes can be more easily rooted out and identity theft becomes more difficult is a valuable contribution to our nation's security and public safety. Of note is that significant cyber protection of such valuable digitized information is essential.

5.2 Physical Security Features

Counterfeiting, tampering and duplication of DLs and IDs are a substantial problem in some states. Manufacturing fake IDs in the United States continues to be a huge business for white and blue collar criminals, alien smugglers, identity thieves and even amateur college students whose clients are not yet of age to enter adult establishments. Setting standards for physical security features of the cards that make creating fakes substantially harder will help ensure greater economic security and public safety, enhancing the ability of law enforcement to catch fakes and discouraging criminals from creating them at all. This includes making the machine-readable technology more secure and the visible data requirements minimized and available only to law enforcement.

Today, technology exists that can merely scan a machine-readable strip on the back of an ID and determine its legitimacy based purely on the content of information in the strip and without accessing any other personal information on the ID. Requiring a machine-readable strip or another of the many available security features with a minimum of defined data elements will help all compliant states determine legitimate versus illegitimate IDs in a variety of law enforcement and public safety contexts.

5.3 Identity Verification

The crux of the 9/11 Commission recommendation on secure DLs and IDs is that we must assure that people are who they say they are. Insufficient information exists to verify identities at present, and the inability of states to do so during the issuance process is arguably the most persistent problem in DL/ID issuance.

Law enforcement officers who deal with all forms of crime, including underage drinking and driving, need DLs/IDs to contain accurate information. Today, 47 states are verifying Social

Security Numbers. However, a common platform should be followed that includes a biometric—in this case a digitized photo—proof of date of birth, address verification and Social Security information.

Determining the authenticity of insecure 'breeder' documents, the most common being the birth certificate, is extremely difficult. In many states, the birth certificate itself is produced at the county and private institution level, and central state records are not maintained, making its authenticity extremely difficult to determine. States relying on such documents are not always aware of the inherent risks but have no alternative at present. Creating a highly protected system of digitized birth certificates, and improving the issuance processes of birth certificates, will go a long way to helping create sub-strata of secure IDs used in the state-issuance of DLs/IDs. Three states have digitized their death and birth records and have piloted a verification system; to date, reports are that these pilots are effective.

For other states, however, it is valuable to simply create the requirement that identities be verified. If, for example, 18 of the 19 9/11 hijackers seeking DLs had simply known that their identities would be verified prior to issuance of DLs or IDs, they likely would have been discouraged from even attempting to get the DLs/IDs in the first instance. Simply asking states to check an automated database that merely gives them a 'yes/no' on the authenticity of supporting identity documents would go a long way to discouraging bogus applications.

CUSTOMER#:   A69600380
CUST. NAME: AL GHAMDI,AHMED,SALEH S
ISSUE DATE: 2001/08/02 12:32
PRINT DATE: Sun Sep 23 10:26:25 EDT 2001

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

Richard D. Holcomb
Commissioner

This ends transmission.

Ahmed al Ghamdi's photo as it appeared on his Virginia ID card upon presentation of a false residency certificate on August 2, 2001. Hani Hanjour, Khalil al Mihdhar, Ziad Jarrah, Abdul Aziz al Omari, Majed Moqed, and Salem al Hazmi also obtained Virginia IDs cards fraudulently, a process begun in

each instance by using false residency information.[27] This digital image was used in successful Eastern District of Virginia prosecution of the individuals who conspired with the hijackers to obtain the IDs. The work done on this case has now evolved into the creation of the ICE DBFTFs.

5.4 Lawful Presence

Those legally within the United States should be able to obtain state-issued DLs and IDs. Legality may be evidenced by either U.S. citizenship or legal non-immigration or immigration status. It makes sense that those immigrants who are eligible include applicants for asylum, refugees, and lawful permanent residents. Virginia has statutory language for 'legal presence' in place. New York, Florida, California and nearly 30 other states have laws requiring U.S. lawful presence to acquire DLs and IDs. Today, over 20 states are already checking the legal status of their applicants.

5.5 State Maintenance and Security of Identity Records

There is an understandable real lack of uniformity in how and for how long states maintain 'breeder' documents such as birth certificates that are used as proof of identity in an application for a DL or ID. Some state motor vehicle administrations destroy documents after just a few months, resulting in an inconvenience for applicants that time and again have to produce the same documents and losing potentially key information for law enforcement attempting to track a multitude of criminal activity from identity theft to organized crime. While digitizing these documents will require immense efforts to gather them at county and state levels and then file and protect the data digitally, these same efforts will yield immensely important resources for identity protection and verification. The numerous scams to obtain legitimate DLs and IDs through fraudulently produced 'breeder' documents will find their ability to do so circumscribed when the documents they are producing can easily be determined by fakes when cross-checked with actual data.

In terms of the security of IDs, counterfeiters and identity thieves must increasingly depend on more sophisticated equipment and covet blank un-issued ID cards. A solid policy supporting better physical security of such facilities, along with personnel trained in fraud and subject to background checks and security clearance procedures to reduce the risk of insider corruption, helps assure an otherwise sound system is not subject to insider manipulation. States are increasingly considering moving to a central location for DL/ID production and distribution to reduce the risk of document theft and burglary.

5.6 One Driver, One License

There is no sound reason for any person of legal stature to hold and use more than one DL or personal ID. The 9/11 hijackers took multiple advantage of their ability to attain multiple state-issued DLs and IDs, claiming to lose them soon after acquiring them and then using a duplicate to acquire a DL or ID in another State. By 9/11, the pilots all had DLs or IDs from more than one state. The Pentagon pilot, Hani Hanjour, had four. Bad drivers, criminals and other terrorists such as al Marabh, discussed previously, all take advantage of such loopholes continually. Criminals and bad drivers also routinely exercise this practice of obtaining

---

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

multiple licenses in multiple states for their respective illegal purposes, which this requirement will correct.

Old IDs must be confiscated if new ones are sought, and the prior state should be notified that the old ID is no longer in use. The U.S. Department of Transportation, through AAMVA, has established a sophisticated system for verifying "one driver – one license" for commercial DL (CDL) holders, but can't determine how many non-CDL licenses those drivers may possess. So in the absence of an "all driver pointer system," there is no way for a state to accurately verify whether an applicant has more than one DL or ID. Names vary; state systems cannot crosscheck each other to verify the existence of other DLs or IDs, so applicants are accepted almost wholly on face value.

States have been aware of this problem since the late 1990s and have sought to cure the multi-DL problem by developing protocols that are spelled out in what is known as the Driver License Agreement (DLA). The DLA puts in place a network of states' driver records for ensuring a 'one driver one license' rule that would network all states' driver records together. While some states have adopted the DLA, the effort to get it ratified in all states is still nascent.

Section 6. Evolution of Identity Security Document Legislation

The 9/11 Final Report recommendations on terrorist travel called for action to "set standards for the issuance"[28] of state-issued IDs, including DLs, and "design a comprehensive screening system addressing common problems and setting common standards with system-wide goals in mind."[29] The ease with which the hijackers acquired these IDs—with no system in place that required identity verification—was viewed as a continuing and significant vulnerability unless states are certified to meet minimum standards for records' safekeeping, issuance, processing of driver licenses and IDs.

The 9/11 Commission findings resulted in AAMVA's creation of a Special Task Force on Identification Security that reported in 2004 that loopholes identified by the Commission exist and must be closed, and made specific recommendations as to the elements of DL issuance that were later reviewed and, for the most part, adopted by Congress. These standards are referred to as the DL/ID Security Framework.[30]

---

[28] 9/11 Final Report, p. 390.

[29] Ibid. at p. 387.

[30] AAMVA's framework is extensive, and Congress drew extensively from this work in drafting its identity security legislation. Most of what is proposed in REAL ID is thus not new to the States or AAMVA, but standards these interested parties were seeking to meet prior to Congressional action.
Identification Security - DL/ID Security Framework
AAMVA DL/ID Security Framework
Appendices
01-4.1-03   FDR Training Program and Materials -- Pending
02-4.2-03   White Paper on Issuing Systems (Over-the-Counter, Central and Hybrid)
03-4.3-03   Driver Licensing and Identification Business Processes - Risk Areas and Control Assessment
04-4.3-03   Internal Controls Best Practices
04-4.5-03   Privacy Principles
06-5.1-03   Framework for Audit Plan
07-6.2-05   U.S. Acceptable Verifiable Resource List
08-6.2-05   Canadian Acceptable Verifiable Resource List
09-6.2-03   AAMVA Board of Directors Resolution 03-08: Use of Foreign Consular Cards for
                   Identification Purposes

In November 2004, Congress passed the Intelligence Reform and Terrorism Prevention Act of 2004 (Public Law 108-458) in an attempt to implement many of the 9/11 Commission's findings of fact and recommendations and the more specific standards detailed in the AAMVA Security Framework. Sections 7211 (minimum standards for birth certificates) and Section 7212 (DLs and personal ID cards) were the key provisions dealing with identity document security.

6.1 Birth Certificates

The provision for birth certificates was a key component of the 9/11 Commission recommendations regarding identity security, recognizing that identity security begins with 'breeder' documents, such as birth certificates, that are often required for purposes of verifying identity in order to attain other documents such as DLs. With no standardization and no system for processing birth certificate issuance in the United States, the market in fraudulent and forged birth certificates continues to be a significant product in the identity document black market.

Section 7211 set the foundation for establishing a system for, in the birth certificate issuance, requiring the Secretary of Health and Human Services (HHS) to issue minimum standards for use of birth certificates by federal agencies that included anti-counterfeiting document production and application processing procedures, identity verification, alongside flexibility in state compliance. The HHS Secretary was also to award grants to states to meet federal standards in proportion to the 'estimated average annual number of birth certificates issued by all the States.' The legislation created another grant category for those states attempting to computerize their birth and death records and developing the capability to match those records within and among the States.

10-6.3-03	Social Security Number Verification Best Practices
11-6.3-03	Address Verification Best Practices
12-6.3-03	Third Party Services for Verification Best Practices
13-6.3-03	Verification Matrix
14-7.1-03	Name Collection, Use and Maintenance Procedures
15-7.2-03	End of Stay and DL/ID Expiration Procedures
16-7.2-03	AAMVA Board of Directors Resolution 03-09: Position on Issuing Driver's Licenses to Undocumented Aliens
17-7.3-05	Personal Identification -- AAMVA International Specification -- DL/ID Card Design Version 2.0, 2005
18-7.4-03	Business Requirements for the Unique Identifier
19-7.4-03	Final Report -- Phase 1: Technical Capability of Biometric Systems to Perform 1:300m Identification (International Biometric Group)
20-7.4-03	Structured Decision Making Roadmap for the Evaluation of Biometric Technologies in a Driver's License Environment (Fischer Consulting Inc.)
21-7.4-03	Biometric Technology Information Needs (Fischer Consulting Inc.)
22-7.4-03	Guidance to Jurisdictions Considering Biometric Technology in Interim
23-7.4-03	Technology Assessment Phase II: Assessment of Alternative Technologies and Unique Identifiers
24-7.4-03	Digital Image Exchange Pilot Project -- Pending
25-8.1-03	Model Legislation: Minimum Penalties and Sanctions for Unlawful Application and/or Use of DL/ID Card
26-8.2-03	Model Legislation: Limiting Information Collection and Use of Machine-Readable Technology
27-8.3-03	White Paper on Data Sharing Between Law Enforcement and Motor Vehicle Administrations

See http://209.85.165.104/search?q=cache:5DdglcqP_gcJ:www.aamva.org/KnowledgeCenter/Driver/SecurityFraud/securityframework.htm+DL/ID+security+framework&hl=en&ct=clnk&cd=1&gl=us&client=firefox-a

6.2 Drivers' Licenses and Personal ID Cards

Section 7212 vested minimum standard negotiated rulemaking authority for DLs and ID cards in the Secretary of Transportation, in consultation with the Secretary of Homeland Security and an undefined group of stakeholders. The law delineated what information was to appear on state-issued DLs and IDs as well as mandated that physical security features and machine-readability be embedded in cards to prevent tampering, counterfeiting or duplication. The regulations also had to include application and card processing procedures; identity documents accepted for verification; and document verification procedures. Section 7212 did not require that state-issued IDs be limited to those lawfully present and also included a negotiated rulemaking requirement that diluted the DHS and State roles in promulgating regulations that remained focused on security as opposed to other special interest priorities.

6.3 REAL ID Act of 2005

In an attempt to make identity security more robust and timely, Congress repealed Section 7212 of the 2004 Intelligence Reform Act in 2005 and replaced its contents with the REAL ID Act of 2005 (PL 109-13) signed into law May 13, 2005.[31] The crux of REAL ID—passed and funded on a bipartisan basis[32]is that it improves national and economic security and public safety by creating a system that for the first time enables identities to be verified. The act also creates common standards for the security of state-issued DL and ID cards and the information on DL and ID cards. These include standards that require:

- o   minimum data visible on DL and ID cards such as full names;
- o   verification of 'breeder' identity documents such as birth certificates, Social Security numbers, and primary residence;
- o   physical security features embedded in the card to protect privacy and make tampering more difficult;
- o   security of manufacturing facilities and background checks for employees handling DL/ID applications and cards;
- o   lawful presence and a match of length of stay to length of DL/ID term;
- o   digitization and maintenance of certain application information; and
- o   a 'one driver/one license' requirement.

REAL ID sets out minimum standards for DL and ID issuance and requires that states that choose to comply provide electronic access to their motor vehicle databases if their state residents are to have access to federal facilities. The law does not bind states. Rather, REAL ID makes clear that noncompliant DLs or noncompliant state-issued ID cards cannot be used for identification for any federal purpose. The law binds federal agencies, not states, thus

---

[31] Public Law 109-13, Section 206. Section 7211 pertaining to birth certificate issuance remains in effect. REAL ID clarifies the legal relationship between federal laws governing definitions such as 'driver's license' and 'identification card'; state issuance; and record-keeping requirements while excluding HAZMAT licenses and other commercial truck driver's licenses already subject to driver license issuance regulation.

[32] In the House, Representative Sensenbrenner (R-WI) and Representative Davis (R-VA), then Chairmen of their respective Judiciary and Government Reform Committees, were primarily responsible for helping REAL ID come to fruition. In the Senate, Senators Judd Gregg (R-NH) and Robert Byrd (D-WV) gave the initial $40 million appropriations.

providing an opt-out for states while making clear that states that choose to opt-out will be inconveniencing their residents who need access to federal facilities for certain purposes.[33] Since REAL ID is not binding on states it is, in fact, less prescriptive in some ways than prior mandates on the states in regard to DLs. These laws all recognize that individual access to a DL poses certain risks to public safety, and the federal government has a strong interest in assuring safety of its residents. For example, regulations already exist regarding requirements for handling 'driving under the influence of alcohol,' including suspension of driving privileges.

Driver safety and driver safety training as a precursor to DL issuance are both detailed in law and regulation. Other rules require that DLs be required to carry visual features so that learner's permits and DLs can be easily distinguished. The National Driver Register (NDR) Problem Driver Point System was founded in a 1982 law directing states to share information about `bad drivers' through this system. Like REAL ID, participation in the NDR is optional and conditioned by federal grants. Yet all 50 states and the District of Columbia participate in the NDR.

Under the Act, DL/ID regulations are drafted by the DHS in consultation with the Secretary of Transportation and the states, while certification for compliance rests solely with DHS.

Section 7. Why Identity Document Security Now

Fraudulent travel and identity documents are a worldwide problem, which will continue to challenge law enforcement officials in the United States and abroad. As long as identification is required to travel and obtain goods or services, criminals will attempt to produce fraudulent documents. [P]riority must be given to the continued development of stronger travel and identification documents. The development and distribution of quality documents [truly resistant to fraud] will be expensive, as it will require replacing old document production systems and infrastructure; however, the investment will pay healthy dividends in security.[34]

Mike Everitt, Forensic Document Lab Unit Chief, Immigration and Customs Enforcement
Testimony, Senate Finance Committee, August 2006

Identity document security is the underpinning of the border recommendations made by the 9/11 Commission. Establishing that people are who they say they are and are entitled to the benefit they seek—whether entering or staying in the United States—is fundamental to protecting both the nation and individuals from those that seek to do us harm. The state DL issuance agencies as represented by their association, AAMVA, recognized the value of these recommendations when it issued its DL/ID Security Framework. Congress further recognized the value of the Commission recommendations and the good work of the states and AAMVA when it passed into law Section 7212 of the 2004 Intelligence Reform Act.   When it became clear that the language in that law needed repair to be effective, the REAL ID Act was passed and signed into law in May 2005. However, REAL ID was only provided $40 million in funding with $3 million released for development. The FY08 contains no budget line for REAL ID. States who choose to comply must do so by May 2008.

---

[33] REAL ID Act, Section 201.

[34] Michael Everitt, Unit Chief ICE Forensic Document Laboratory, DHS. Testimony before Senate Finance Committee, *Border Insecurity, Take Two: Fake IDs Foil The First Line of Defense.* August 2, 2006.

As this is written in February 2007, the final Notice of Proposed Rule Making is apparently imminent. DHS Undersecretary for Policy Stewart Baker and Assistant Secretary for Policy Development Richard Barth are currently working with the Office of Management and Budget to finalize the proposed rules for release for comment. Meanwhile, criticism grows amongst states and privacy advocates with varieties of arguments that dismiss the law's value to national security while raising issues pertaining to privacy and cost. Furthermore, the 9/11 Commission is defunct. Those responsible for getting REAL ID passed have lost their committee chairmanships and H.R. 1, which is described as the 110th Congress' 9/11 Commission implementation legislation, does not even acknowledge REAL ID nor how important identity security was to the 9/11 Commission recommendations. Continually, others seek its delay, repeal or renegotiation.

Under these circumstances, REAL ID will likely meet an uneven implementation at best. That is not the way to secure America. Embedding identity security into state-issued DL/ID systems will take significant planning to fulfill the requirements of REAL ID and significant financial resources for the 'brick and mortar' start-up costs. Congress must step up to the plate and make securing of identity documents the national priority that our citizens deserve.

We cannot forget the national security significance of terrorists like the 9/11 hijackers assimilating into the United States by attaining 17 driver licenses from Arizona, California and Florida and 13 state-issued IDs from Florida, Virginia and Maryland. The hijackers then used those IDs for the purpose of renting cars, obtaining living quarters, opening bank accounts, and boarding aircraft. At least six hijackers presented state-issued IDs to airline employees on the morning of 9/11. Nor can we consider insignificant the economic and public safety considerations of document rings like the Castorena family that cost identity theft victims and financial institutions millions and millions of dollars, let alone a clientele who use their fake IDs for any number of illegal and dangerous purposes. Making identity more secure squeezes the counterfeiter and the end-user, making both more vulnerable to law enforcement and making us all safer as a nation.

The 9/11 Final Report recommendations on terrorist travel called for action to "set standards for the issuance" of state-issued identifications, including DLs, and to "design a comprehensive screening system addressing common problems and set common standards with system-wide goals in mind." The ease with which the 9/11 hijackers acquired state IDs—with no system in place that required identity verification—will continue to be a significant vulnerability unless states are certified to meet minimum standards for the safekeeping and issuance of records and the processing of driver licenses and IDs.

In December 2005, the 9/11 Commissioners gave Congress a good mark for passing into law solid language pertaining to its identity security recommendations in the 2004 Intelligence Reform Act and 2005 REAL ID Act. However, the Commissioners remained concerned with the states' ability to comply, stating: "The REAL ID Act has established by statute standards for state-issued IDs acceptable for federal purposes, though States' compliance needs to be closely monitored." Building state competency in this area will be at best incomplete if states fail to receive the necessary federal funds for establishing an identity security system within and between their jurisdictions.

All states and the federal government rely on the quality of state documents, meaning our national security is at risk until all states implement systems to ensure that applicants are who they claim to be and have a legitimate status in the United States.

In addition, a comprehensive system to improve the quality of the vetting and issuance system for state-issued IDs will provide benefits for Americans far beyond national security. Identity security means less opportunity for those who seek to fraudulently acquire or forge state-issued identifications for nefarious purposes, including traditional white and blue collar crime, scam-artists and identity thieves, dead-beat dads, and even teenagers trying to purchase alcohol. Over the past couple of decades, Congress has mandated rules on HAZMAT DL issuance, drunk drivers, driver safety training, and information sharing on problem drivers—all in the federal interest of public safety.

A first significant step in enhancing our national and economic security and our public safety is within our grasp if Congress is willing to partner with the states and invest adequately in identity security systems. This nation should support the many good efforts in many states to infuse credibility and reliability into our most basic identity documents and issuance systems. A good place to start is by asking Congress to provide states with $1 billion in "one time upfront costs" to comply with regulatory requirements to be issued in 2007 to facilitate identity document security improvements. The National Governors' Association, the National Conference on State Legislatures, and AAMVA developed this request after completing a comprehensive evaluation of the upgrades and new procedures that likely will be required in jurisdictions around the country.