U.S. House Homeland Security

Subcommittee on Border, Maritime and Global Counterterrorism

"Moving Beyond the First Five Years: Using the Western Hemisphere Travel Initiative to Implement Common Sense Border Security"

April 16, 2008

Testimony of Janice L. Kephart

Former Counsel, 9/11 Commission

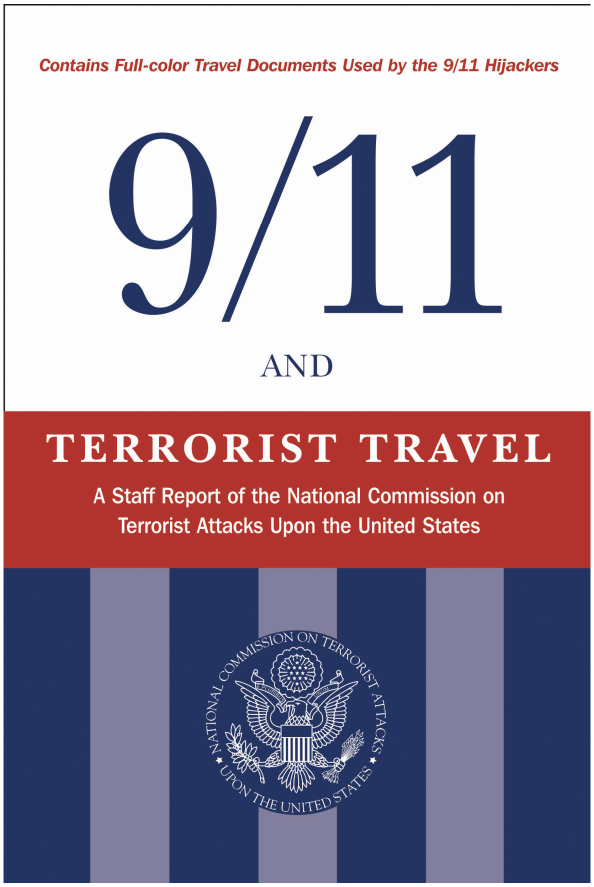
President, 9/11 Security Solutions, LLC

911securitysolutions.com

Introduction

Chairman Sanchez, Ranking Member Souder. Thank you for having me here today. It is an honor to be here. I appreciate very much this committee's continued interest and effort in the 9/11 Commission recommendations, including the issue of identity document security that the Western Hemisphere Travel Initiative, REAL ID and Enhanced Driver Licenses addresses head-on. Without assuring that people are who they say they are, and that the documents they present are legitimate at our borders and within our borders, we have done little to nothing to contain what me and my team mates on the 9/11 Commission termed 'terrorist travel'.

I am here in my own capacity today, but you should know that when the 9/11 Commission issued its final report card in December 2005, one of the highest marks it gave was to Congress for passing *REAL ID* legislation that set minimum standards for the issuance of state-issued driver licenses (DL) and IDs.[1] I am also happy to be one who speaks with the 70 percent of Americans who, in a Zogby/UPI poll from late last year, are in favor of secure driver licenses. Like REAL ID, the *Western Hemisphere Travel Initiative* (WHTI) fulfills a 9/11 recommendation that called for the presentation of a passport or equivalent for all persons seeking entry into the United States.


Contains Full-color Travel Documents Used by the 9/11 Hijackers
9/11
AND
TERRORIST TRAVEL
A Staff Report of the National Commission on Terrorist Attacks Upon the United States
NATIONAL COMMISSION ON TERRORIST ATTACKS UPON THE UNITED STATES

The *Enhanced Driver License* and State Department issued *PASS Cards* will assure citizenship while providing a cost-effective way to facilitate travel for those living and working on our land borders. These alternative forms of ID for the border satisfy the Commission's recommendation that other, 'equivalent' documents, might be sufficient for border inspection. As long as these documents are able to be checked for fraud, citizenship, and against derogatory information to the extent passports are today, I can say with confidence that the Commission would consider them acceptable for entry today. *Trusted traveler programs* such as NEXUS, SENTRI and the Global Entry programs are essential to such systems, to help assure high (not low) risks are the focus for border inspectors.

One crucial caveat remains: *national standards for birth certificates*- made a legal requirement in 2005- and *digitization of birth (and death) records* are pivotal to verifying identity for other government issued IDs, including REAL IDs and e-passports. While states are making progress in digitizing birth and death records, continual building of the Electronic Verification of Vital Events system needs to remain a priority. Where states are partnering with the federal government to digitize records, huge dividends are being found in the fraud fight in health care, but hooking this information in for DMVs and other legitimate uses will provide the essential foundation to the secure ID framework upon which all these programs ultimately rely.

[1] In addition, I have written three papers on the subject. The most recent was published in February 2008. *REAL ID: Final Rule Summary* takes the 280 page Final Rule and summarizes it in nine pages. The second paper from April 2007, *Identity and Security: REAL ID in the States,* answers policy concerns being echoed in some states regarding REAL ID implementation. This paper remains salient, as criticisms of REAL ID implementation are answered, and some of these criticisms are still heard today. The third I published in February 2007 and sets out the policy backdrop for the REAL ID Act, explains its content, and discusses what is at risk if it fails. *Identity and Security: Moving Beyond the 9/11 Staff Report on Identity Document Security* emphasizes the need for security at the base of the nation's identity document issuance processes.

Terrorist Travel and Passports

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

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

We know 9/11 operational ringleader Mohammad Atta used his training as well to manipulate passports to hide travel and substitute information that would leave a fraudulent trail of less suspicious travel. We also know that the recently assassinated Mugniyah of Hezbollah supplied his members with travel documentation as needed.

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

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

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

Until WHTI comes into full implementation at all U.S. border crossings, terrorists with Canadian, Caribbean or Mexican citizenship—or those that pose as such-- can move in and out of the United States right virtually unconcerned about detection. There are legitimate concerns about both the northern, southern and sea borders. The Western Hemisphere Travel Initiative thus becomes an important first step in at least chilling terrorist travel between the U.S. and Canada/Mexico and the Caribbean. This includes any variety of terrorist, whether a Mexican Islamic convert (as sought out by Al Qaeda) or Canadian.[2] Terrorists do not like to be detected or detectable, nor do they want their identity "frozen". (We know, for example, from detainee reporting after 9/11, that the tightening of immigration admission standards for persons traveling from countries of interest resulted in Al Qaeda leaders seeking out young recruits and others with easy access to the West—U.S. citizens, Canadians, Mexicans and those with access to Visa Waiver passports that would not be subject to biometric entry requirements.)

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

The staff report I co-authored with my 9/11 Commission border teammates, *9/11 and Terrorist Travel,* details in even greater depth how the 9/11 hijackers exploited our vulnerabilities using our legal border system. Part of the everyday business of terrorist travel is the bustling black market in doctored and false passports. In addition, an estimated 10 million lost or stolen passports or national identification cards worldwide afford terrorists easier access to world travel.[3] This permits easy travel based on aliases, fake or stolen identities that, at a land border, may or may not be subject to a database check. Requiring U.S. citizens to carry a passport or biometric equivalent also means U.S. border inspectors no longer need to play a guessing game as to who is and who is not a U.S. citizen. On the Canadian and Mexican sides of the border, having a combination of the standard passport or equivalent and registered traveler programs that limit what a border officer must review gives border officers a better chance of snuffing out Canadian, Mexican or other Western Hemisphere passports or 'equivalents' that might be fake or stolen.

Terrorist Travel between the U.S. and Canada

Until WHTI is fully implemented, terrorists with Canadian citizenship can move in and out of the United States virtually unconcerned about detection. It has long been known—and I testified extensively to this fact in 2005 and 2006 before both Houses of Congress—that Al Qaeda recruiters targeted youths with U.S., Canadian or Western European passports, solid English language skills and an understanding of these cultures. A couple of years ago FBI reported these efforts were resurging. Plenty of examples of terrorists seeking or accessing the United States based on Canadian residency or citizenship, or illegally:

[2] For more information about the threat of Canadian terrorist entry over the northern border, see my testimony of November 17, 2005 before the House Small Business Committee, "Building a Wall Between Friends: Passports to and from Canada?"

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

- Jabarah brothers who were recruited to blow up the Singapore harbor but were caught by authorities after swearing allegiance to bin Laden;
- 9/11 mastermind KSM's affiliate Abderraouf Jdey who was initially slated to take part in a second wave of attacks after 9/11;
- Ahmad Said Al-Khadr was bin Laden's highest ranking associate in Canada and raised a family sworn to allegiance to Al Qaeda; a high-ranking ranking Al Qaeda operative who had emigrated to Canada from Egypt in 1975;
- Mohammed Warsame attained U.S. residency after becoming a naturalized Canadian citizen and moved to Minneapolis in 2002. He was arrested in December 2003 as a material witness in the Zacarias Moussaoui case.
- Hizballah cigarette smuggling scam operated for over the U.S.-Canadian border for over a decade with single truckloads sometimes yielding $2 million. Profits were used to buy dual use military equipment and sent back to Hizballah high command in Lebanon. Credit card and banking scams in Canada provided funding, and the Canadian section reported directly to Hizballah's military procurement officer in Lebanon.

- Nabil Al-Marabh tried to illegally enter the United States near Niagara Falls by hiding in the back of a tractor-trailer in June 2001. He had a forged Canadian passport and fake social insurance card.[4] He later told authorities he had regularly traveled illegally between Canada and the United States.[5] Moreover, Michigan state records showed Al-Marabh receiving five driver's licenses there in thirteen months; he had licenses for Massachusetts, Illinois, Ontario, and Florida,[6] and a commercial driver's license and a permit to haul hazardous materials,[7] including explosives and caustic chemicals.[8] In 2002, he pled guilty to conspiracy to smuggle an alien into the United States[9] and was ordered deported.[10] Prosecutors said the government had no evidence linking him to terrorism.[11] The judge questioned the government's previous documentation of Al-Marabh's ties to terror and also noted he was found with $22,000 in cash and $25,000 worth of amber jewels in his possession when he was arrested.[12] He was deported to Syria in January 2004 for his strong ties to the Jordanian Millenium plot.

Seventeen Canadian citizens and residents were arrested in Toronto on June 3, 2006 for terrorist conspiracies across southern Ontario, including subway systems and the Parliament Building in Ottawa. Found in their possession were three tons of ammonium nitrate, 1-½ times that used in the 1995 Oklahoma City bombing responsible for 168 deaths. The arrests were only the second time Canada has used the Anti-Terror law passed after 9/11.

The LA Times reported that the FBI has been working closely with the Canadians on the case, and that the Canadian cell received visits from two terror suspects arrested in April 2006 from Georgia, Syed Haris Ahmed, a 21 year old Georgia Tech student and naturalized U.S. citizen, and Ehsanul Islam Sadequee, a 19 year old Fairfax, VA native**.**   They had met at an Atlanta mosque. The men, according to U.S. court documents, had been in email

[4] Dimmock, Gary and Aaron Sands. "Toronto Shop Clerk Tied to World Terror." The Ottawa Citizen. Oct. 29, 2001.
[5] Ibid.
[6] Schiller, Bill. "Terrorism Suspect had Florida Link." Toronto Star. Oct. 26, 2001.
[7] Philip Shenon and Don Van Natta Jr., "U.S. Says 3 Detainees May Be Tied to Hijackings," *The New York Times*, November 1, 2001.
[8] Wilgoren, Jody and Judith Miller. "Trail of Man Sought in 2 Plots Leads to Chicago and Arrest." New York Times. Sept. 21, 2001.
[9] USA v. Al-Marabh. WDNY 01-CR-244-A. Plea Agreement. July 8, 2002.
[10] Fainaru, Steve. "Sept. 11 Detainee is Ordered Deported." The Washington Post. Sept.4, 2002.
[11] Ibid.
[12] Owens, Anne Marie. "Judge Gets No Answers on Syrian: Former Toronto Suspect Jailed in U.S. for Border Breach." The National Post. Sept. 4, 2002.

communication with the Canadian cell and physically went to Canada to meet in early March via Greyhound bus from Atlanta to discuss U.S. attacks and receiving military training in Pakistan. (The two men had already conducted surveillance, including in Washington D.C.)[13] Both the Canadian cell and the U.S. suspects were in internet communication with each other and suspected terrorists abroad, including a London cell arrested shortly thereafter. Over the internet, a variety of plots focusing on the U.S. Capitol, the World Bank, fuel storage facilities and aviation towers were discussed.[14]

The reporting on the Canadian plot does not mention whether there are any immigration records for the two Georgia men on their entry into Canada or their return into the United States.

Ahmed Ressam of the LAX Millenium Plot[15] used a false French passport to travel to Montreal where he lived for the next four years. In Canada he "became interested in going to bin Laden's camps for training" after "friends returned to Montreal with stories about Osama bin Laden's 'Jihad University' in Afghanistan."[16]

In April 1998, after meeting with Abu Zubaydah in Pakistan, Ressam was sent to the Khalden camp in Afghanistan where he spent the next five to six months. Khaldan had earned a reputation for its instruction in how to acquire, forge, and manufacture travel documents and credit cards, and Ressam learned well.[17] At Khaldan Ressam also learned the other tradecrafts of a terrorist, the use of weapons, bombmaking, and urban warfare.

Zubaydah himself was sufficiently impressed with Ressam's passport manipulation abilities to have apparently asked him to acquire additional Canadian passports for distribution to al Qaeda fighters.[18] And it was Ressam's deft handling of fake travel documents that brought him to the attention of Khalid Sheikh Mohammed during his final visit to Pakistan. He would soon return to Canada (in January 1999) to pursue the plot to blow up Los Angeles International Airport.

On December 14, 1999, a sweaty, nervous Ahmed Ressam was given a secondary inspection when he became reluctant to answer a basic question about his destination. He had just pulled off from a late-arriving ferry at Port Angeles, Washington. In answer to questions, Ressam pulled out fake documents—including a Canadian passport- in the name of Beni Antoine Noris. This was not the first time Ressam was asked questions. Ressam had already undergone a cursory examination by a U.S. immigration officer in Vancouver, who had been suspicious of Ressam as he was the last to board an already late ferry. The examination included a cursory look in the trunk (but not the tire well where the explosives materials were hidden) as well as a run of the name on the passport (Noris) against the INS terrorist database without getting a hit. Although a subject by the name of Ressam was wanted in Canada, neither that name nor the alias Noris was in the INS database. Ressam was admitted for boarding.

[13] Jason Chow and Ricardo Alonso-Zaldivar, "Canada Arrest 17 in Alleged Terror Plot." *Los Angeles Times*, June 4, 2006.

[14] Ibid.

[15] Most of this section was attained while I was counsel on the 9/11 Commission, with supplemental research provided by Vinay Tripathi while I was a senior consultant for the Investigative Project on Terrorism on a to date unpublished report entitled "An In-Depth Analysis of the Structure of Al Qaeda and Militant Islamic Terrorist Groups in the United States: The Enterprise of Terror in the United States" (March 2005).

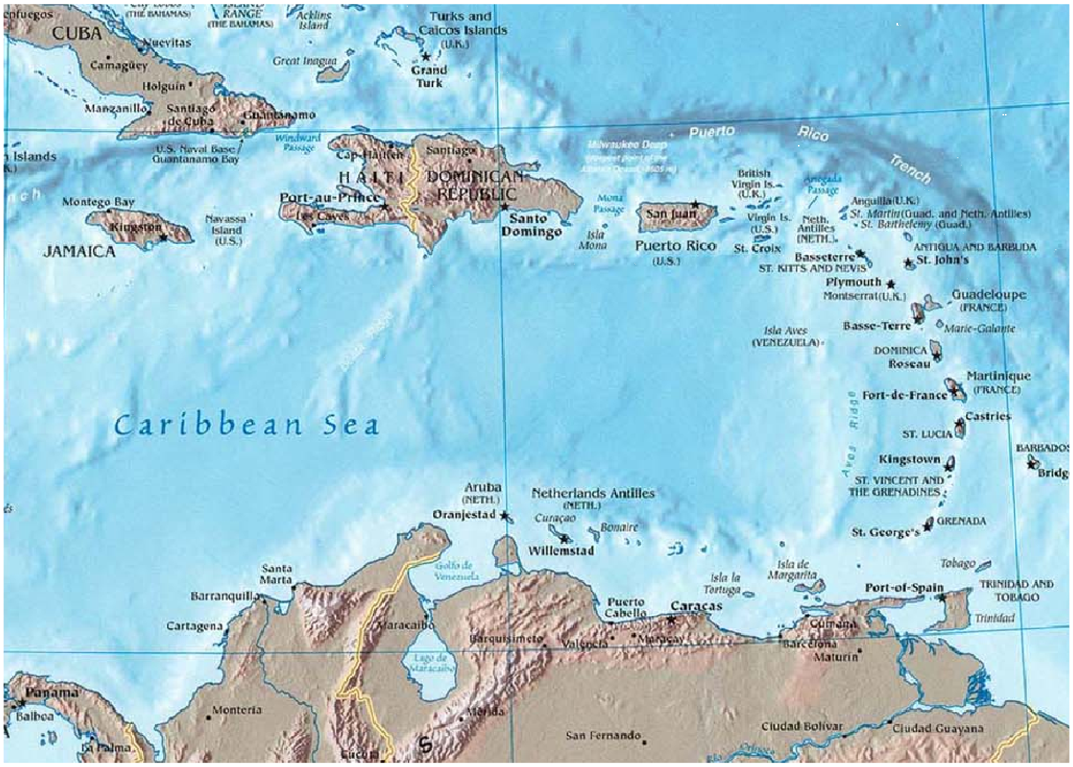
[16] "Trail of a Terrorist: Introduction." PBS FRONTLINE. Oct. 25, 2001 http://www.pbs.org/wgbh/pages/frontline/shows/trail/inside/cron.html

[17] USA v. Ressam, et al. WDWA 99-CR-666. "Indictment." April 3, 2001. *See also* Zill, Oriana. "Crossing Borders: How Terrorists Use Fake Passports, Visas, and Other Identity." Documents." Frontline. October 2001. http://www.pbs.org/wgbh/pages/frontline/shows/trail/etc/fake.html; and USA v. MOKHTAR HAOUARI, et al. SDNY S4 00 Cr. 15. Cross-examination of Ahmed Ressam, July 3, 2001 (transcript p. 549-551).

[18] Zill, Oriana. "Trail of a Terrorist: Crossing Borders: How Terrorists Use Fake Passports, Visas, and Other Identity Documents." PBS FRONTLINE. Oct. 25, 2001 http://www.pbs.org/wgbh/pages/frontline/shows/trail/etc/fake.html

Ressam's trial testimony provides valuable insight into one terrorist's ability to circumvent border security around the world. He described how al Qaeda supplemented its global terrorist network with operatives trained in Afghanistan and thereafter embedded in satellite locations. In France, Canada and elsewhere, Ressam operated in conjunction with fellow terrorists stationed in Europe. He traveled extensively using doctored travel documents that allowed him to take on a variety of identities, including the one he used in Canada—that of a refugee seeking asylum and a new home. In actuality, Ressam was a member of the Armed Islamic Group[19] (GIA, or Groupes Islamiques Armés).

Ressam testified that manufacturing and trafficking fraudulent travel documents served several functions, providing entrée to the target country, a means to make money, and a way to stay embedded in a given location. From 1994 to 1998, Ressam lived in Montreal, actively robbing tourists—some thirty to forty times, by his count—of money and travel documents. Ressam described his livelihood: "I used to take the money, keep the money, and if there [were] passports, I would sell them, and if there [were] Visa credit cards, I would use them up, and if there were any traveler's checks, I would use them or sell them."[20] Though Ressam was arrested four times for his thievery, he was convicted just once; and he was punished with a fine, not jail time.[21]



Trinidad and Tobago is on lower right. Below is Venezuela. Antigua and Barbuda is mid-right.

Terrorist Travel between the U.S. and the Caribbean

Trinidad and Tobago, a rich tourist island located off the northeast coast of Venezuela, had a failed attempted Islamic extremist coup in July 1990. Fifteen percent of the island is Muslim. The island is also to the immediate

[19] Zill, Oriana. "Crossing Borders: How Terrorists Use Fake Passports, Visas, and Other Identity Documents." Frontline. October, 2001. http://www.pbs.org/wgbh/pages/frontline/shows/trail/etc/fake.html

[20] USA v. Ressam, et al. WDWA 99-CR-666. "Indictment." April 3, 2001.

[21] Ibid.

northeast of Venezuela, which has long flaunted its contempt of the United States and support for terrorist activity, including reported travel facilitation to terrorists.

In June 2007, four men, three from Guyana (sharing a southeast border with Venezuela) and one from Trinidad were arrested for their plot to destroy fuel lines that support JFK International Airport. One of the suspects reportedly said the airport was picked due to the esteem held in the U.S. for John F. Kennedy. The FBI was involved with the case since January 2006, when one of the four alleged plotters, Russell Defreitas, unknowingly attempted to recruit an FBI informant in an attack within the United States. Its goal was to be more spectacular than September 11. Defreitas had previously been a baggage handler at JFK airport and assured his co-conspirators that he knew the airport intimately.

"This was a very determined group that engaged in precise and extensive surveillance, surveillance that included physical surveillance, photograph surveillance, video surveillance, and even the use of the Internet to obtain satellite photographs of the JFK facility," according to FBI agent Mershon who had investigated the case.

Abu Bakr is a former policeman who founded the violent Jama'at al Muslimeen (commonly referred to simply as the Jamaat). A Trinidad native, he formed the group after studying in Canada where he converted to Islam while a student there. His group attempted a coup against the Trinidad government in 1990. The group, especially with Abu Bakr as leader, had a close relationship to Libyan leader Muammar al Qaddafi. Most recently, after threatening violence and extortion against fellow Muslims, he was convicted in March 2006 for attempted murder of former organization members. A search of his headquarters found a cache of weapons and equipment. He was long considered to be a crime kingpin in Trinidad, and his rivalries spun off a number of other radical Islamic groups.

Other groups active on the island are Waajihatul Islaamiyyah (The Islamic Front) and the Jamaat al Murabiteen. The Waajihatul Islaamiyyah group has links to al Qaeda, Hamas, Egyptian Islamic Jihad and Jemmah Islamiyyah, the organization behind the Bali beachfront bombing that killed close to 200 people. In December 2002, the FBI, CIA and British SAS agents were in Trinidad investigating separate reports about specific plans to attack local U.S. and British interests by the head of The Islamic Front, Umar Abdullah, who had reportedly been threatening U.S. and British interests on the island.

Abdullah publishes a monthly newsletter that pontificates on behalf of Osama Bin Laden, Al Qaeda, the Taliban, a "Jihad" (Holy War) against the US and Britain and the setting up of an Islamic State here.

There were also reports prior and subsequent to 9/11 U.S.-sought Adnan El-Shukrijumah was living in Trinidad near schools that share his last name. (I had evidence while on the Commission that El-Shukrijumah may have tried to help 9/11 pilots Atta and Jarrah with an immigration matter at the Immigration offices in Miami in May 2001. See *9/11 and Terrorist Travel*, p. 30-31) In addition, two men with ties to Trinidad have been arrested in the United States. Keith Andre Gaude, a Jammat linked to bin Ladin, pled guilty on September 19, 2001 to unlawful possession of a machine gun. BATF officials stated he had come to Florida to "buy as many as 60 AK-47 assault rifles and 10 MAC-10 submachine guns with silencers."

In 2002, Trinidad native and U.S. naturalized citizen Shueyb Mossa Jokhan was sentenced to 58 months in federal prison for a "jihad" mission that included bombing an electrical power station and a National Guard Armory. According to the FBI, "these attacks were then to be followed by a list of demands to be placed on the United States government and other governments around the world. The defendants also sought to acquire AK-47 type assault weapons for their jihad training and operations, and sought to obtain the release from custody of an individual described as a "mujahedin" fighter committed to jihad."

Since 9/11, there have been reports of Al Qaeda members setting up shop in Trinidad, smuggling weapons and organizing cells.

Antigua and Baruba were the home of John Lee Mohammed prior to his ten fatal shootings and three other near fatal shootings during a terrorist-style spree in the autumn of 2002. As a U.S. citizen, he had financially survived prior to coming to the United States by selling forged U.S.-accepted travel documents—driver's licenses and birth certificates. [22]

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

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

After the Task Force created by the Attorney General of Antigua and Baruba released its Final Report in December 2002, the GAO released two 2003 studies about the ease of being admitted into the United States with counterfeit birth certificates and driver's licenses from Canada, Mexico, Jamaica and the Bahamas. According to the GAO, the ease of fraudulent entry using something other than U.S. passports for those claiming U.S. citizenship was not limited to Muhammed and his clients.

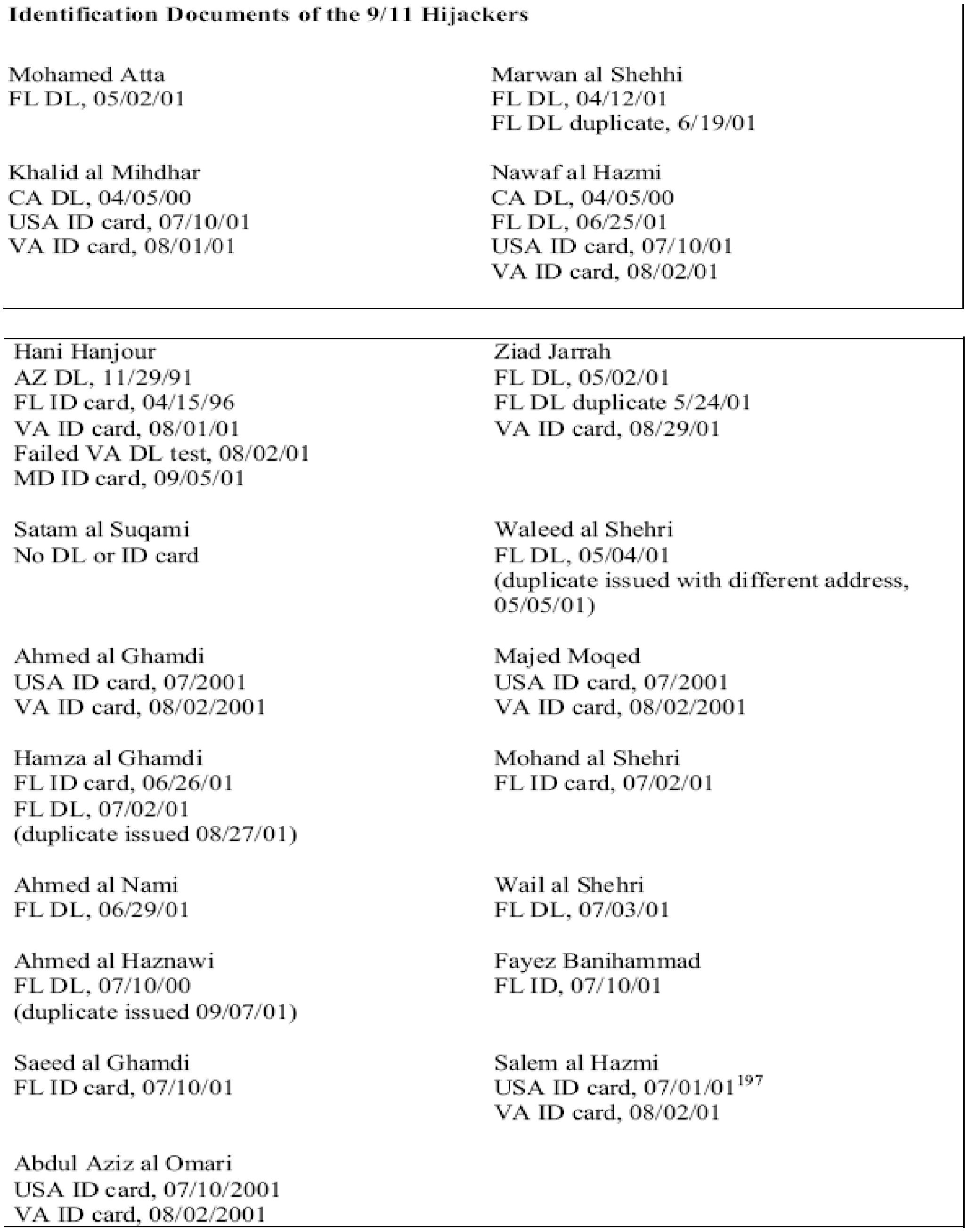
Terrorist Travel and State-Issued Driver Licenses and IDs

The 9/11 hijackers assimilated into the United States by attaining 17 DLs from Arizona, California and Florida (four of which were duplicates) and 13 state-issued IDs from Florida, Maryland and Virginia. The hijackers then used those IDs for the purpose of renting cars, obtaining living quarters, opening bank accounts, and boarding aircraft on the morning of 9/11. We know that at least six hijackers total presented state-issued IDs on the morning of 9/11. The pilot who flew into the Pentagon, Hani Hanjour, had ID cards from four states: Florida, Maryland and Virginia, and an Arizona driver's license. The Pennsylvania pilot, Ziad Jarrah, had three IDs and an unverifiable ID when stopped for speeding two days prior to 9/11. Both pilots had obtained a Virginia ID by fraud.

At the foundation of the 9/11 Commission 'terrorist travel' recommendations on secure IDs was the basic understanding that terrorists will continue to easily assimilate within the United States as long as identity and identity document issuance processes are easily manipulated. The Commission stated:

> 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 DLs.
> **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. (p. 390, 387)

[22] *Antigua and Barbuda Final Report of Task Force Investigation of John Allen Williams, a.k.a John Allen Mohammad*. (Dec. 2003).



Identification Documents of the 9/11 Hijackers

Mohamed Atta FL DL, 05/02/01	Marwan al Shehhi FL DL, 04/12/01 FL DL duplicate, 6/19/01
Khalid al Mihdhar CA DL, 04/05/00 USA ID card, 07/10/01 VA ID card, 08/01/01	Nawaf al Hazmi CA DL, 04/05/00 FL DL, 06/25/01 USA ID card, 07/10/01 VA ID card, 08/02/01
Hani Hanjour AZ DL, 11/29/91 FL ID card, 04/15/96 VA ID card, 08/01/01 Failed VA DL test, 08/02/01 MD ID card, 09/05/01	Ziad Jarrah FL DL, 05/02/01 FL DL duplicate 5/24/01 VA ID card, 08/29/01
Satam al Suqami No DL or ID card	Waleed al Shehri FL DL, 05/04/01 (duplicate issued with different address, 05/05/01)
Ahmed al Ghamdi USA ID card, 07/2001 VA ID card, 08/02/2001	Majed Moqed USA ID card, 07/2001 VA ID card, 08/02/2001
Hamza al Ghamdi FL ID card, 06/26/01 FL DL, 07/02/01 (duplicate issued 08/27/01)	Mohand al Shehri FL ID card, 07/02/01
Ahmed al Nami FL DL, 06/29/01	Wail al Shehri FL DL, 07/03/01
Ahmed al Haznawi FL DL, 07/10/00 (duplicate issued 09/07/01)	Fayez Banihammad FL ID, 07/10/01
Saeed al Ghamdi FL ID card, 07/10/01	Salem al Hazmi USA ID card, 07/01/01[197] VA ID card, 08/02/01
Abdul Aziz al Omari USA ID card, 07/10/2001 VA ID card, 08/02/2001	

State-issued IDs acquired by 9/11 hijackers, "9/11 and Terrorist Travel", p. 44

As the 9/11 Commission noted, there was only one 9/11 hijacker who did not obtain some form of U.S. identification, whether a state-issued DL, personal ID or both. Three of the five hijackers who crashed a plane into the Pentagon used fraudulently obtained licenses to board. The pilot of that plane had four IDs, all from different states, with at least one obtained by fraud. If REAL ID had been in effect in 2001, the 9/11 operational ringleader and pilot that conducted the first World Trade Center suicide, Mohamed Atta, would only have been four days from having had an expired license when he was pulled over for speeding violation on July 5, 2001.

The 9/11 hijackers could have done the same today. It is still possible to obtain multiple licenses and IDs because identities are not verified. It's not only possible to game the system; it's likely, because states still don't exchange information with each other regarding those holding legitimate IDs. Police officers' hands are tied when they can't cross check the ID they've been handed against any other information.

The 9/11 hijackers are not the only terrorists we know of who have taken advantage of blind spots and weaknesses in ID issuance standards. One terrorist caught in 2001 on the northern border, Nabil al Marabh, had five DLs and a hazardous materials permit. He told authorities he frequently crossed the U.S.-Canadian border illegally. Mir Aimal Kansi, who killed two people outside CIA headquarters in 1993, got a Virginia DL despite being in the U.S. illegally. These same problems exist in many states today. As long as they do, terrorists will continue to take advantage of them.

In addition to terrorists, criminals of all ilks – identity thieves, counterfeiters, deadbeat-- and even underage teens seeking IDs to drive and drive, also use multiple IDs to hide their true identity from the law. In 2005 identity theft costs were at a staggering $64 billion, with $18.1 billion of that cost involving theft of a DL or ID. Individual consumers spend an average of 330 hours trying to undo identity theft and suffer $15,000 on average in losses. With REAL ID, identity theft will be much more difficult due to more robust, secure ID verification systems will protect consumers from identity thieves both during the application process and once the DL or ID is issued.

The cards themselves will also be less susceptible to alteration, with three levels of security making the cards more tamper-resistant and easier for law enforcement to determine fakes. Counterfeiting remains alive and well. The accompanying photo is from a November 2007 New York press conference whereby state and federal authorities from seven different law enforcement agencies shut down six ID document mills in New York and made at least 128 arrests. The bust covered two criminal enterprises that together took in more than $1.5 million annually. Typical street price was $40 - $60. The ring supplied fraudulent government identity document such as DLs, Social Security cards and resident alien cards. Suppliers were located in California and New York and forged documents from many states, Central America and Mexico.

Nov. 2007: New York State investigators alongside federal authorities make arrests pending a two year investigation of two criminal counterfeiting enterprises spanning California to New York.

Annual income was more than $1.5

Of particular note was the 2006 bust of the Castorena Family organization, which beginning in the 1980s operated a Mexico-based counterfeiting operation with cells in every major U.S. city. Annual sales in Chicago alone were $2.5 million. According to informants, they could make IDs "as good as any we carry in our pockets."

The major source for the case, the stepdaughter of the organization's leader, asked her grandfather whether the organization sold to terrorists. She was told: "We do this for business, for money. So it doesn't really count whether you're a Mohammed or a Julio or somebody else, as long as you have the money to pay for it. Terrorism is not our problem."

Western Hemisphere Travel Initiative

The tenets of WHTI were recommended by the 9/11 Commission to both tighten border security and streamline the inspection process, especially at our land ports of entry. We cannot afford our borders be bifurcated from the discussion of national security. Our economic strength as a nation is only as strong as our national security. We must continue to work alongside our friends in the trade and tourism industries to achieve both security and facilitation.

Assuring our border inspection process is fast, fair and complete is essential. It is also doable. We can do so if we prioritize how personnel, budgets and technologies are allotted and deployed with precision. The focus must be on how to properly train and equip our border inspectors so that procedures assure security of our borders are the most effective and least intrusive manner possible. I applaud DHS for not waiting despite continual efforts by special interests to delay implementation indefinitely, even if border inspection has waited for over seven years for the significant upgrades in procedures and processes that should have been in place before 9/11 and forthcoming after 9/11. The new rules set in place for WHTI implements policy that shores up significant, large and sweeping holes in our border security so that all persons seeking entry into the United States show standardized travel documents or equivalents that can be vetted in a manner that assures identity and maximizes facilitation simultaneously.

Remember where we are without WHTI: terrorists, drug dealers and those who abuse our lax security will continue to easily move through our border system with fake documents or no documents at all. The policy which has been in effect for years at our ports of entry, the Western Hemisphere Travel Exception, actually encouraging fraudulent entry by permitting any traveler claiming to be a U.S. citizen to talk their way into the United States or show any variety of identity document and claim to be from the Western Hemisphere. At least on the Canadian border, surveys from even a couple of years ago showed that 40% of Canadians state they have not been asked to show any identification when seeking entry into the United States. In a 2006 GAO report, GAO proved the point when in 42 of 45 instances between 2003 and 2006 GAO agents with counterfeit documents were able to flash false papers, or in a few instances, no papers at all, and enter the United States. Consider that number transferred over to attempted terrorist entries, and we have much to be concerned about until WHTI is fully rolled out.

The only way to secure our borders is to make the terrorists choose between using a passport, and enhanced DL (where available), applying to a trusted traveler program, or enter illegally. As long as a terrorist can pose as a U.S. citizen or traveler from the Western Hemisphere by producing a birth certificate, fake DL that can't be verified, or other forms of identification that can be neither verified for identity, checked against a watchlist, or authenticated as a legitimate document, the Western Hemisphere Travel Exception is an open invitation to enter and embed in the United States with little disincentive not to try.

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

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

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

REAL ID

REAL ID is one of the only 9/11 Commission recommendations that relies heavily on the states for implementation. REAL ID might have curtailed 9/11. REAL ID can make a difference to our national security, our economic security and our public safety – but only if fully implemented and adequately funded. To make REAL ID a reality, however, requires more than either the federal government or the states can do on their own. It requires a partnership. It also requires an acknowledgement that securing our nation's physical and economic integrity is not just a federal responsibility; it is everyone's responsibility. It requires a further acknowledgement that the ability to verify an individual's true identity is one of the cornerstones of national and economic security.

The REAL ID Act stipulates that in order for a DL or state-issued ID to serve as an identity document for entering a federal facility – including boarding a plane – the document must meet, at a minimum, the security standards spelled out in the Act. Thus states are not required to issue licenses and IDs in accordance with REAL ID, but they could be subjecting their residents to considerable inconvenience if they do not. There is no intent under REAL ID for the federal government to assume responsibility for issuing DLs. That process should and will remain with each state. REAL ID seeks only to ensure that every state's process for issuing DLs and IDs – including the documents themselves – meets specified minimum security standards.

Today, the controversy around REAL ID has shifted significantly from one of the value of the law to its funding, and for good reason. With only $79 million available for 50 states and 6 jurisdictions to meet initial compliance deadlines in a year and a half, this Congress needs to take the funding of REAL ID seriously. If ever there was a domestic funding emergency, REAL ID represents one of significance.

Debunking Myths about REAL ID

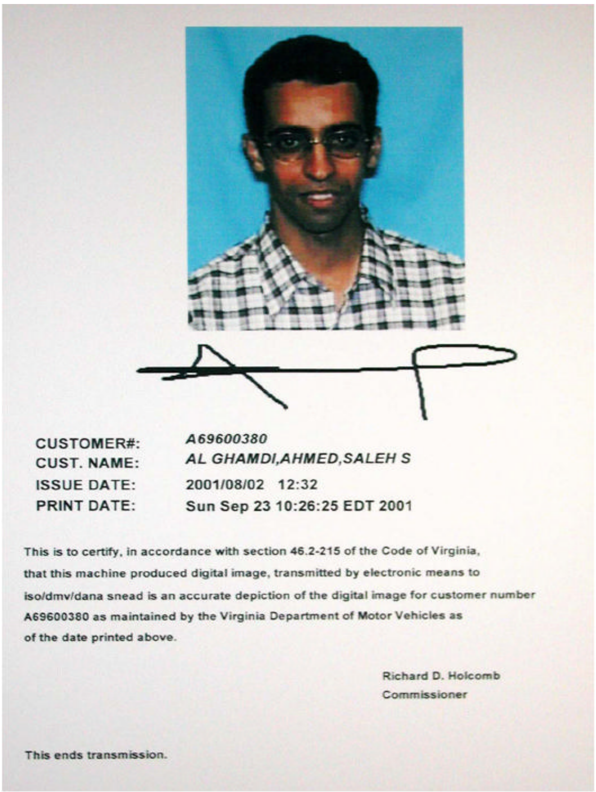
Myth: REAL ID is a federal imposition, with little to no connection to state efforts to improve ID issuance.

Fact: REAL ID was passed into law based on the states' own Secure Document Framework developed by AAMVA after the states acknowledged post 9/11 that the current state DL issuance system is deeply flawed in its ability to generate IDs both secure in their content and production. Such deep weaknesses threaten national and economic security, public safety, and privacy.

On October 24, 2001 the American Association of Motor Vehicles Administrators (AAMVA) – an organization promoting information exchange, uniform practices and reciprocity, with representatives from every US and Canadian jurisdiction – passed a resolution to form a special task force to enhance the security and integrity of the DL and ID issuance processes. AAMVAnet already supported the Commercial Driver License Information System and provides connectivity for such things as SSN checks by DMVs, and AAMVA's leadership in setting standards for bad drivers made them the logical choice for taking on issues related to 9/11.

Prior to 9/11, AAMVA had a significant leadership role that included petitioning Congress in 1996 to mandate minimum standards for DLs. From 1999 to 2001, AAMVA worked with the National Highway Transportation Administration (NHTSA) and Congress towards creation of the Driver Record Information Verification System (DRIVerS). So when AAMVA went to work on creating a special task force to deal with the panoply of issues involved in creating a more secure ID issuance framework, the organization had the ability and credibility to make a difference. And they did. Their work became the foundation for the technical requirements of the REAL ID Act.

The REAL ID Final Rule, issued on January 11, 2008, has responded to 1000s of comments by states and other stakeholders and provided a new set of compliance deadlines which the National Governor Association acknowledges as reflective of their concerns and suggestions. All states are now set up to comply, with all states having been issued an extension to comply with the initial benchmarks set out by the Rule of January 1, 2009 instead of the law's deadline of May 11, 2008. The relaxation of the timeline to comply has resulted in a reduction of estimated costs by DHS from about $11 billion burden on the states to a $3.965 billion requirement spread over 11 years, or about $360 million per year to implement.



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.

9/11 hijacker Ahmed al Ghamdi, shown above, checked in at Logan Airport in Boston on the morning of 9/11, using his fraudulently obtained VA ID card.

The Driver License/ID Security Framework that emerged from the AAMVA Special Task Force was detailed and comprehensive; that Framework became the backbone for REAL ID. The outline of the task force responsibilities is worth repeating as it shows how AAMVA – and thus the state DMVs – were well aware and desirous of fixing the multiple vulnerabilities in state ID issuances systems. In some ways, then, REAL ID was simply a federal bow to the states' own work in this area. AAMVA's 'Uniform Identification Subcommittee' divided the issues into sub-categories. What is interesting is that despite the permutation of the mission statements from these subcommittees to the AAMVA Security Document Framework, to REAL ID, to the Proposed and Final Rule, much of the language and policy statements have remained relatively unchanged.

Another interesting aspect of AAMVA's tasking was a group established just to deal with enforcement issues, including those treating/ID fraud, and determine increased penalties for dealing with such fraud. A significant justification for REAL ID is that by setting minimum standards as a foundation in both the verification of identity and card production processes, security is built into all state systems. This will make law enforcement activity more effective while at the same time discouraging fraud. As Chuck Canterbury, National President of the Fraternal Order of Police stated in a Feb. 21, 2007 letter to Senate Majority Leader Harry Reid:

> [REAL ID] is very much of an officer safety issue. Law enforcement officers need to have confidence that the documents presented to them to establish the identity of a given individual are accurate. Officers rely on these documents during traffic stops and other law enforcement actions to access information related to that individual's criminal history. No police officer wants to be in the dark about the fact that he may have detained a wanted or violent criminal who has simply obtained false identification. This places both the officer and the public he is sworn to protect in greater danger. For this reason, the FOP will strongly oppose any bill or amendment that would repeal the REAL ID Act.

Below is a chart that shows that the policies advocated by the states via AAMVA's 2001 working groups remains a strong influence on REAL ID policies advocated today by DHS and also influenced by the National Governors' Association and National Conference of State Legislators. This chart reflects where AAMVA started in 2001 as closely tied to REAL ID Final Rule.[23]

Secure ID feature tasked by AAMVA	2001 AAMVA Secure ID Issuance Task Force assignments	2008 DHS REAL ID Final Rule for Secure ID Issuance
Model Legislation *Process and Procedures* *Driver License Agreement* *DRIVerS Infrastructure*	'develop model legislation to assist states in implementing the overall package of Uniform Identification Standards' 'gather and incorporate all deliverables of the Uniform ID Subcommittee (Task Groups) into one Model Program. This model program will include minimum requirements, best practices and model legislation to support a uniform and secure DL and identification card system for motor vehicle agencies in the U.S. and Canada.' 'The DLC/NRVC (Driver License Compact/Non-Resident Violator Compact) Joint Compact Executive Board has been asked to explore enhancing the newly created Driver License Agreement (DLA), a voluntary DL compact between States, to include requirements established for a more secure DL/ID issuance system. ' 'The Driver Record Information Verification System (DRIVerS) task group will be charged with creating an all driver pointer system, to keep bad drivers off the road. Simply put, DRIVerS will direct a state where to find and accurately verify someone's driving history in another state.	REAL ID is that legislation. Section 37.01: REAL ID is applicable to States and U.S. territories that choose to issue DLs in compliance with REAL ID, and IDs not in compliance of REAL ID. The Rule sets out minimum requirements to support a uniform and secure DL and identification card system for Motor Vehicle Agencies.
Acceptable Documents	'validate and update the existing acceptable ID document list for the proof/authentication of specific personal information, such as, name, date of birth (DOB), legal presence, etc. and evaluate the utilization of foreign documents for	Sections 37.11 (Identity Verification) and 37.13 (Document Authentication) require that an applicant provide sufficient documentation for a state to verify identity and authenticate documents presented for the purpose of establishing identity and

[23] Janice Kephart, *REAL ID Final Rules: a Summary* (Feb. 21, 2008) was used for column three. Found at http://911securitysolutions.com/index.php?option=com_content&task=view&id=154&Itemid=38

Residency	the same purpose. Phase two will result in a recommendation for document (DL/ID) validity periods in relation to legal status/validity' 'to develop a definition of residency/domicile with and without a legal presence requirement for the purpose of driver licensing (establishment of the driver control record) and identification. '	includes specific personal information such as name, DOB, legal presence and use of documents, including foreign documents, for that purpose. An ID document list is provided. Lawful Presence is defined in 37.03, and the procedure for determining lawful status for the purpose of driver licensing is found in 37.13. Lawful status must be checked in SAVE, Section 37.13(b)(1). The issuance with or without legal presence is covered by Section 37.21, Temporary or Limited Term IDs and in Section 37.71, Non REAL ID DL or ID.
Verification *Fraudulent Document Recognition*	'identify and establish methods for verifying documents used to establish identity of an individual applying for a DL or identification card. Verification of identity may include, but is not limited to, full legal name, date of birth, Social Security Number (when applicable), and residency and/or legal presence' 'to assist jurisdictions with the formal training of motor vehicle employees and law enforcement in the recognition/detection of fraudulent identification documents.'	Again, methods for verifying (authenticating) documents are covered by Sections 37.11 and 37.13. Section 37.31 provides requirements for source document retention. Section 37.33 sets out minimum requirements for information held by DMV databases. Sections 37.41(b)(2) set out security requirements for personally identifiable information. Section 37.41(b)(5) requires employee fraudulent document training and security awareness training.
Card Design Specifications	'deals with physical and encoded features of the DL / ID document. Features include security elements, card layout, printed and encoded data, and machine-readable technologies. It is our hope that this effort produces a standard for the DL document that specifies minimum data and minimum technologies to be used on the DL / ID document'	Section 37.15 sets out minimum security requirements to harden the DL or ID but assures flexibility, based on comments received during rulemaking. Section 37.17 lists card surface requirements and 37.19 the machine readable zone requirement.
Internal Controls	'to identify best practices for internal fraud control and prevention measures'	Sections 37.41 to 37.45 set out controls for physical security of production facilities; employee background checks and access control; requires a state to submit a plan on preventing access to personally identifiable information; and a separate report on safeguarding IDs in coordination with law enforcement.
Oversight Compliance System	'to review current procedures for the oversight and compliance of Federal and State programs and to develop a process for compliance to AAMVA standards regarding DL/ID Processes/Procedures'	Sections 37.51 to 37.65 set out in detail procedures for determining state compliance.

Unique Identifier	‘ developing a way to uniquely identify an individual such that: • A holder will have no more than one (1) DL/ID card and record • authorized users can verify that the holder of a DL/ID card is the individual to whom the card was issued; and • an individual’s driver record contains only information that pertains to that individual.	• Section 37.29 sets out the ‘one driver one license’ rule designed in part to verify driver licensing in another state. This helps get out the underlying principle of “keep bad drivers off the road” as referred to in DRIVerS infrastructure above. • Supported by document security requirements in Section 37.41(b)(2) and source document retention Section 37.31

Myth: REAL ID creates a national ID and is a federal mandate.

Fact: The driver’s license is the most common form of ID used in the U.S. today, accepted for everything from opening a bank account to boarding a plane to picking up movie tickets with a credit card. Securing an already widely used credential makes good sense. Each state will still issue many varieties of REAL ID compliant – and if they choose – non-compliant IDs. REAL ID does not affect states’ right to decide who is eligible for a DL or ID; that decision remains with each state. There is thus nothing “national” about such issuance. If anything, REAL ID can be said to obviate the need for a national ID.

One example of how REAL ID does not create a national ID is that the benchmarks do not mandate anti-counterfeiting features of the card. Instead, under Section 37.15 of the Final Rule, anti-counterfeiting is described as follows:

> 37.15(c) Three levels of security are required to detect false cards:
>
> Level 1 requires an “easily identifiable visual or tactile feature” for cursory examination without any aids.
> Level 2 is a feature detected by “trained inspectors with simple equipment.”
> Level 3 is a feature only detectable by forensic inspectors.

To meet these security levels states have numerous choices from a large variety of vendors. The Rule simply states that the card technologies must not be commonly available to the general public, must be multilayered, and must be able to be integrated into the cards. There is nothing about these requirements that creates one type of card issued by one government entity; in fact, these rules are designed to give states the choices they need to make to achieve fiscal responsibility and security in equal doses.

Myth: REAL ID will create a hackable, national database.

Fact: There is no aggregation of personal data into “one huge, hackable database operated by the federal government,” as some claim**.** REAL ID calls for the states to operate secure databases that are searchable by other authorized parties such as motor vehicle agencies and law enforcement. The Act also calls for crosschecking applicants’ information with federal and state databases to better authenticate credentials. No actual information is shared between these databases, just simply 'yes' or 'no' answers, and there is no access to the actual information that stands behind queries.

Further, the federal government does not hold applicants' information; in fact, the REAL ID Final Rule requires that applicant information be protected by each state. Nor does the federal government network the databases together. The databases are likely to be networked to the states by an AAMVA secured network, for which DHS has requested FY09 funding of $50 million for further upgrades. Most of these databases are currently used by states already to verify identity in a variety of ways – with no privacy complaints. Thus the federal government will not hold individual applicants' information, and the notion that REAL ID would create a single federal database is completely erroneous.

***Myth: REAL ID invades privacy*.**

Fact: REAL ID protects privacy by ensuring that people are who they say they are. The information contained on a REAL ID license will be the same as what is required by most states today. That information, such as a digital photo, name, permanent address, age, height and weight, is widely available and does not implicate privacy concerns. REAL ID licenses are not required to contain RFID technology, biometric fingerprint information, or Social Security numbers.

The Final Rule supports privacy of personal information in a number of areas, including protection of personally identifiable information; access to information by employees; and securing production facilities.

Best practices on securing privacy have existed in the DL arena for years and build on the Commercial Driver License Information System (CDLIS) and National Driver Register (NDR) database created in 1986. These databases together have been servicing 45 states for 20 years, and REAL ID does not even go so far as creating a new database. Even so, there have been no complaints about intrusions on privacy or identity theft with either of these databases. One reason why is because federal law already protects the use of such data under the Driver's Privacy Protection Act of 1994. This law restricts how DL information can be used by states, barring states and their employees from selling or releasing personal information such as SSNs, images, addresses, phone numbers and birthdates. Until that law was passed, 35 states had such information public and many made money off the sale of such information to all varieties of private enterprise. Congress set a higher bar to protect privacy in the area of state-issued DLs then, and REAL ID 20 years later is a natural follow-up: not only securing data, but identities and the documents that support those identities as well.

Also worthy of mention is that the Information Technology Association of America, who represents the largest producers of computer security systems—IBM, Microsoft, Hewlett Packard, Oracle and others—has concluded that REAL ID, if implemented, will further protect privacy. In a May 7, 2007 report, the ITAA stated that REAL ID will actually "raises the bar on privacy for driver licenses" because it sets higher benchmarks for data security; requires tougher identity adjudication; and builds on existing practice.

REAL ID also provides greater protection of privacy, requiring background checks of DMV employees, secure productions sites of cards, alongside due respect to civil liberties. Just to be clear, there are no plans for an embedded RFID chip in REAL ID DLs. Enhanced DLs are a different species, designed for border crossers who also regularly use a DL, and who voluntarily choose to acquire an Enhanced DL with a chip readable for border crossing purposes.

Myth: The opportunities for identify theft will multiply exponentially.

Fact: A collateral positive side effect of REAL ID is that it will help curtail identity theft, not enable it. For legal residents, REAL ID requires stronger security features with the intention of driving up the cost of creating counterfeit ID documents and enabling law enforcement both working with DMVs and in the field to make a quicker, more reliable determination of whether an ID is legitimate or not.

For criminals, terrorists and others who want to live in the U.S. for nefarious purposes or under false guise, obtaining a license or ID has been their ticket to acquiring legitimate cover for their illegitimate activities. Once our identity issuance systems and the IDs themselves are tightly secured, it will be much more difficult to obtain these "tickets" fraudulently.

FUNDING REAL ID

A review of the Final Rule shows that the administration request does not adequately reflect the costs in the Final Rule as they pertain to state investment in order to become REAL ID compliant. That is the crux of the current debate. Six years after 9/11, we can no longer afford delays simply due to funding when acceptable rules are in place.

After collecting thousands of comments from states and other interested parties, the Department of Homeland Security (DHS) issued final rules for the REAL ID Act in January 2008. All 56 U.S. jurisdictions meet initial REAL ID requirements and as of April 2, 2009, have been granted an extension until December 31, 2009 by the DHS. That means that every jurisdiction will continue to have their DLs acceptable for official purposes after the May 11, 2008 deadline as mandated by Congress in the REAL ID Act of 2005.

Funding for REAL ID under these circumstances is wholly inadequate. While Congress provided additional funding to implement REAL ID in FY08 at $50 million, current REAL ID funding is at approximately $79 million in a separate fund created under the REAL ID Act for all U.S. jurisdictions.

The DHS Final Rule places the cost to the states at $3.965 billion. With an 11 year implementation cycle, states need on average $360 million per year to fund full REAL ID under their own estimates.

In FY09, the administration made a request to fund REAL ID at a total of $160 million, with $50 million going to USCIS for the identification verification 'hub' that is likely to be expanded by AAMVA (as of now). The administration has made a separate request for a combined grant program for critical infrastructure/bomb prevention and REAL ID of $110 million. This proposed fund is neither dedicated to REAL ID nor does it reflect the costs to the states as set out by the Final Rule. Here is the relevant language as set forth by the administration:

OMB FY09 proposed budget numbers, p. 480

> CITIZENSHIP AND IMMIGRATION SERVICES, Federal Funds, UNITED STATES CITIZENSHIP AND IMMIGRATION SERVICES
> For necessary expenses for citizenship and immigration services, ø$80,973,000¿ $154,540,000; of which $100,000,000 is for the E-Verify program to assist U.S. employers with maintaining a legal workforce; and of which *$50,000,0000 is to support implementation of the REAL ID Act to develop an information sharing and verification capability with States*.
>
> p. 516 National Security and Terrorism Prevention Grants *($110 million).*— This program provides competitive grants to specific State and local agencies to support proposals *which address national vulnerabilities identified by the Secretary as priorities. In 2009, the Secretary will invite States to submit project proposals to support REAL ID implementation* and buffer zone protection for critical infrastructure. *Final grant allocations will be determined competitively by the Secretary on the basis of how well proposals address identified national vulnerabilities.*

In a March letter to the White House, the National Governors' Association (NGA) requested $1 billion on 2008 spring supplemental, citing compliance deadlines beginning in 2009. In addition, a group of seven governors has told Secretary Chertoff that they want complete funding for REAL ID in the supplemental this spring of $1 billion: REAL ID is an emergency, as all states seeking compliance or approved for an extension (all but one so far) need to reach 18 benchmarks by January 2009. Most are well on their way, but many lack sufficient funding to reach all 18 benchmarks by this date.

ESTIMATED COST OF REAL ID FINAL RULE OVER AN 11-YEAR PERIOD[24]

Estimated Costs (11 years)	**$ million**	**$ million**	**$ million (2006 dollars)**	**% Total**
	7% discounted	**3% discounted**	**undiscounted**	**Undiscounted**
Costs to States	**2,879**	**3,413**	**3,965**	**39.9%**
Customer Services	636	804	970	9.8%
Card production	690	822	953	9.6%
Data Systems & IT	1,171	1,352	1,529	15.4%
Security & Information Awareness	365	415	490	4.9%
Data Verification	5	7	8	0.1%
Certification process	11	13	16	0.2%
Costs to Individuals	**3,808**	**4,814**	**5,792**	**58.3%**
Opportunity Costs	3,429	4,327	5,215	52.5%
Application Preparation (125.8 million hours)	2,186	2,759	3,327	33.5%
Obtain Birth Certificate (20.1 million hours)	348	440	530	5.3%
Obtain Social Security Card (1.6 million hours)	31	37	44	0.4%
DMV visits (49.8 million hours)	864	1,091	1,315	13.2%
Expenditures: Obtain Birth Certificate	379	479	577	5.8%
Cost to Private Sector	**8**	**9**	**9**	**0.1%**
Costs to Federal Government	**128**	**150**	**171**	**1.7%**
Social Security card issuance	36	43	50	0.5%
Data Verification - SAVE	9	11	14	0.1%
Data Systems & IT	65	74	82	0.8%
Certification & training	17	21	25	0.3%
Total Costs	**6,853**	**8,406**	**9,939**	**100.0%**

The total, undiscounted eleven-year cost of the final rule is $9.9 billion. Based on a total of 477.1 million issuances over the 11-years of the analysis, the average marginal cost per issuance for States is $8.30. Individuals will incur the largest share of the costs. More than 58 percent of the costs (discounted or undiscounted) are associated with preparing applications, obtaining necessary documents, or visiting motor

[24] Source: DHS Final Rule, p. 221. http://www.dhs.gov/xprevprot/laws/gc_1172765386179.shtm

vehicle offices.

The final cost to states and the federal government at $4.4 billion for complete implementation of REAL ID. States have to be compliant by 2011, leaving only three fiscal years for reaching benchmarks set out for DHS, although the final implementation date is 2017.

According to the federal government, their burden is priced at $171 million.   These costs cover Social Security Card issuance ($50 million); Data Verification via SAVE ($14 million); Data Systems & IT ($82 million); and certification and training ($25 million).