Testimony
Richard C. Barth, Ph.D.
Assistant Secretary for Policy Development
Department of Homeland Security

Before the
Senate Committee on Homeland Security and Governmental Affairs
Subcommittee on Oversight of Government Management, the Federal Workforce, and the District of Columbia
On
Understanding the Realities of REAL ID: A Review of Efforts to Secure Drivers' Licenses and Identification Cards
03/26/2007

Chairman Akaka, Senator Voinovich and distinguished Members of the subcommittee, thank you for the opportunity to appear before you today to discuss REAL ID.

As you know, REAL ID is based on a recommendation of the 9/11 Commission. It is a recommendation to deter future terrorist acts that the Department of Homeland Security (DHS) strongly supports. Versions of this Act have passed Congress, twice: first, as part of the Intelligence Reform and Terrorism Prevention Act of 2004; and then, as the REAL ID Act of 2005.

> On page 390 of its final report, the 9/11 Commission stated:
>
> "Secure identification should begin in the United States. The federal government should set standards for the issuance of birth certificates and sources of identification, such as driver's 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 that people are who they say they are and to check whether they are terrorists."

All but one of the 9/11 hijackers acquired some form of U.S. identification document (ID). The remaining 18 hijackers fraudulently obtained 17 drivers licenses and 13 state issued identifications, and some even possessed duplicate driver's licenses. The pilot who crashed American Airlines Flight 77 into the Pentagon, Hani Hanjour, had ID cards from three states. The driver's licenses and state IDs enabled the hijackers to maneuver throughout the United States in order to plan and execute critical elements of their mission. Using these documents, they were able to rent cars, travel, take flying lessons and board airplanes. The 9/11 hijackers evidently believed that holding driver's licenses and ID cards would allow them to operate freely in our country. And they were

right. The hijackers viewed U.S. driver's licenses and ID cards as easy and convenient ways to become "Americanized."

The 9/11 hijackers are not the only terrorists operating inside the U.S. to have used fraudulently obtained IDs. The terrorist who killed two employees outside CIA headquarters in 1993, Mir Aimal Kansi, also exploited the loopholes in getting a driver's license. He was present illegally as a visa overstay, but was still able to obtain a valid driver's license.

Congress's recognition of the significant vulnerabilities in our current state systems of issuing driver's licenses led to the passage of the REAL ID Act.

The Department believes that the 9/11 Commission's REAL ID recommendation is one of the linchpins of our entire national security strategy. Counsel to the 9/11 Commission, Janice Kephart, said the recommendation was "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" (*Identity and Security*, February 2007, page 1). Said another way, identity document security is a foundational layer for security in the United States. If we cannot verify that people are who they say they are and if we allow loopholes in obtaining driver's licenses and IDs to exist, DHS's job and that of law enforcement becomes exponentially more difficult. We know of instances where law enforcement pulled over one or more of the terrorists, then let them go. Sadly, four of the hijackers had been stopped for traffic violations in various States while out of legal immigration status.

As required by statute, DHS proposed for public comment REAL ID regulations that would create minimum standards for State driver's licenses and identification cards issued on or after May 11, 2008. Under this proposal, States must certify that they are in compliance with these requirements, and DHS must concur, before the driver's licenses and identification cards that the States issue may be accepted by Federal agencies for specified official purposes. Because DHS recognizes that not all driver's licenses and identification cards can be reissued by May 11, 2008, the proposal provides a five-year phase-in period for driver's license or identification card renewals. The proposed rule also includes an extension through December 31, 2009, for States requesting it. Therefore, all driver's licenses and identification cards that are intended to be accepted for official purposes as defined in these regulations must be REAL ID licenses and identification cards by May 11, 2013.

Key features of the proposed rule include the following:

- Applicant documentation. States would require individuals obtaining driver's licenses or personal identification cards to present documentation to establish identity – U.S. nationality or lawful immigration status as defined by the Act, date of birth, social security number (SSN) or

ineligibility for SSN, and principal residence. States may establish an exceptions process for the documentation requirement, provided that each such exception is fully detailed in the applicant's motor vehicle record.

- Verification requirements. States would verify the issuance, validity, and completeness of a document presented. This proposal specifies electronic verification methods depending on the category of the documents.
- Information on driver's licenses and identification cards. The following information would be required to appear on State-issued driver's licenses and identification cards: full legal name, date of birth, gender, a unique driver's license or identification card number (not the SSN), a full facial digital photograph, address of principal residence (with certain exceptions), issue and expiration dates, signature, physical security features and a common machine-readable technology (MRT).
- Security features on the card. The proposal contains standards for physical security features on the card designed to prevent tampering, counterfeiting or duplication for a fraudulent purpose, and a common MRT with defined data elements.
- Physical security/security plans. Each State must prepare a comprehensive security plan for all state Department of Motor Vehicle (DMV) offices and driver's license/identification card storage and production facilities, databases and systems and submit these plans to DHS as part of its certification package.
- Employee background checks. States would conduct name-based and fingerprint-based criminal history records checks against State criminal records and the FBI's National Crime Information Center and Integrated Automated Fingerprint Identification System, respectively, on employees working in State DMVs who have the ability to affect the identity information that appears on the driver's license or identification card, who have access to the production process, or who are involved in the manufacture of the driver's licenses and identification cards. States would pay a fee to the FBI to cover the cost of each check. States would also conduct a financial history check on these employees.
- State certification process. Similar to Department of Transportation regulations governing State administration of commercial driver's licenses, States will be required to submit a certification and specified documents to DHS to demonstrate compliance with these regulations and demonstrate continued compliance annually.
- Database connectivity. States would be required to provide all other States with electronic access to specific information contained in the motor vehicle database of the State. States would have to verify with all other States that an applicant does not already hold a valid REAL ID in another State.

As demonstrated by the details of the proposed rule, REAL ID is not a national identification card and it does not create a national database. It is, however, a

network-of-networks. All 50 States and U.S. territories are asked to meet a minimum standard of security for issuing state drivers licenses and IDs. Some States may opt to do more to enhance security. They will be given the flexibility to do that. And it is the States, not the Federal government, that will collect and store the information submitted to support issuance of the card as is the current practice. Furthermore, States will have the option of issuing non-REAL ID drivers' licenses if they choose.

REAL ID is a collaborative process with the States and territories. The NPRM reflects input from States and territories, including the extension for States which was previously touched upon. Secretary Chertoff announced on March 1st that States may use up to 20% of their Homeland Security Grant Program funds to comply with REAL ID. Again, here the Department is flexible and eagerly awaits further input by the States and territories during the comment period.

REAL ID is technically feasible. As you will see by the appended chart – "System Connectivity by State" – there is already widespread activity being undertaken throughout the country by States to improve their standards for issuing ID cards. In accordance with the proposed rule, States would be required to do checks against four databases before issuing a REAL ID license or identification card. Some States are already beginning to do checks against these databases. Forty-eight of the fifty States and the District of Columbia are connected to the SSOLV (Social Security On-Line Verification) database operated by the Social Security Administration. Twenty States are using the SAVE (Systematic Alien Verification for Entitlements) database operated by DHS, and the vast majority of the remainder have entered into memoranda of understanding to work with DHS toward SAVE participation on or before May 11, 2008. In FY06, participating State DMVs ran 1.2 million queries against the SAVE System. Three States are involved in a pilot with National Association for Public Health Statistics and Information Systems (NAPHSIS) to check birth certificates via the EVVE (Electronic Verification of Vital Events) database and seven States already are responding to EVVE requests. Finally, the State Department will be developing the system to permit DMVs to check electronically that a passport an individual presents to the DMV has been lawfully issued. Work here is still ongoing, but we have been fully engaging with State on this important matter.

Returning to the issue of Social Security number verification, a recent state audit report showed 27,000 people in North Carolina used bogus Social Security numbers when applying for a driver's license or state ID. About half of these belong to persons that are shown as deceased in SSA records. This report highlights the security need for crosschecking the databases required under REAL ID.

At the end of the day, what does all this look like? While the rule is still pending, there is no definitive answer quite yet. However, the final answer is that the REAL ID standards will likely draw from all the best and most secure State practices already in place. Critics have charged that there are privacy issues connected with the requirement to verify an individual's data. However, three of the four systems are already used by the States. In addition, the NPRM only requires State-to-State data exchange for those who possess a REAL ID license. This mandate simply extends data exchange requirements already successfully implemented in the Commercial Driver's License Information System (CDLIS). Decades ago, Congress enacted the Commercial Motor Vehicle Safety Act of 1986 to improve highway safety because prior to the Act, commercial drivers were able to obtain multiple licenses from different States, allowing persons to hide convictions and unqualified applicants to get licensed. CDLIS has eliminated this security problem successfully and has not had any privacy breaches since it began. In fact, once the program was up and running – during a four-year period from 1992 to 1996 – an estimated 871,000 commercial motor vehicle operators were disqualified. With the potential of multiple licenses hiding convictions, etc. many of these drivers could have continued driving "under the radar screen" of law enforcement and escaped detection by States.

If the system the Department of Homeland Security proposes with REAL ID denies just a few bad actors, from hiding behind fraudulent identities, what a boon to national security that would be. And, at a minimum, it makes it tougher for terrorists to do their job. It destabilizes a sure-fire method employed by the 9/11 hijackers as well as other terrorists to become, as they perceived, "Americanized" simply by holding a license that grants broad entry and unlocks many doors in our society.

The 1986 Act also prompted motor carriers all across the country to strengthen safety departments and employee training programs. Much the same is true of REAL ID, which requires DMVs to train their employees to spot faulty documentation and stop terrorists or other criminals from exploiting loopholes that currently exist in obtaining a driver's license or state ID.

There have been concerns voiced about REAL ID creating a national identification card and national database. These concerns are simply not true. The proposed rule maintains the existing practices of how information is stored, collected and disseminated at the State and local level. The fact remains that REAL ID does not give the Federal government any greater access to the information than it had before.

States and territories would be required to include a Comprehensive Security Plan to show how information will be safeguarded, including procedures to prevent unauthorized access or use, and procedures for document retention and destruction. Additionally, DHS would require each state to submit a privacy policy.

Contrary to some press reports, DMV employees would not be able to "fish" around through other State or territory databases for personal information. Nor does the proposed rule require radio frequency identification (RFID).

Another aspect of privacy is encryption of data in the networks and of data on the cards. Since most States and territories do not encrypt information contained in their 2D barcodes, the Department does not require it in the proposed rule. DHS is seeking recommendations from the States, territories, and privacy community regarding the need for encryption as well as cost-effective ways to deploy it while still providing access to critical information to law enforcement. We do favor encryption of data flowing over the networks. We will be working with our partners, the States, to deploy the right solution that protects privacy while avoiding heavy costs on the States. Good encryption protection generally requires frequent re-keying of the encryption codes. While this is feasible for the networks carrying data between various Federal and State agencies, it appears to us at this time to be infeasible for the data stored on that cards that must be accessible to law enforcement officials.

The Department has been working with the privacy community on areas of common interest to protect personal information. Corruption within DMVs can sometimes be a problem. To give you a few examples, two DMV employees in Connecticut were charged in December of 2004 with stealing licensed drivers' identities in order to issue fake driver's licenses to illegal immigrants. In the same case, the identities of two males were stolen to commit credit card and bank account fraud in the amount of $15,000. At that same time, a New York ring was uncovered where five DMV employees were selling fake IDs for up to $4,000 apiece. Three buyers were illegal immigrants from Pakistan.

We believe REAL ID has benefits beyond national security. One such benefit is the prevention of identity theft. The system of gathering and verifying information and issuing REAL ID cards will make it much more difficult for document counterfeiters and identity thieves to steal identity from unsuspecting citizens and obtain a valid REAL ID card. A more stringent process in place for obtaining a driver's license will add a layer of defense in the fight against identity theft. Currently, it's all too easy to perpetrate identity theft and cross-checking vital documents prior to issuing a license will help crack down on this behavior.

There are many ways for a resourceful thief to commit identity theft. Some common forms of identity theft that could include use of a fraudulent driver's license are: bank fraud, employment-related fraud, evasion of legal sanctions, medical fraud, insurance fraud, and house and apartment rental fraud. These types of identity theft accounted for a significant percentage of all reported incidents in 2005. The total U.S. cost of identity theft in 2005 was $64 billion, of which $18.1 billion was for theft involving a license, as we document in the economic impact analysis published with the proposed rule. A more recent

survey by the Council of Better Business Bureaus *(2006 Identity Fraud Survey Report, Javelin Strategy & Research)* found that roughly 8.9 million U.S. adults were victims of identity theft in 2006. Just resolving the theft cost for the average victim was approximately $422 and took 40 hours. Applying the average wage rate at that t time (i.e., $17 per hour), the economic value of the time victims spent just resolving identity theft has been nearly $10 billion. These figures were used by the Department in the Economic Analysis for REAL ID. But don't just take our word for it. A study by the Identity Theft Resource Center *(Identity Theft: The Aftermath 2004)* found that victims spent an average of 330 hours to recover from identity theft. Forty percent of the victims reported losses greater than $15,000. Regardless of which way you slice it, the loss of time and money is significant. These studies do not even include the mental duress victims go through, which must be significant.

Widespread acceptance of REAL ID as required identification could have other benefits as well, such as reducing unlawful employment, voter fraud, and underage drinking.

Initial issuance of REAL IDs will present challenges. However, for people who are organized and have their birth certificate, social security card and marriage certificate all in one place, it will not be unduly inconvenient. And, to be frank, we think spending a little more time at the DMV is a price worth paying to enhance our security. As Americans, we've made sacrifices every day since 9/11.

Any State or territory that does not comply increases the risk for the rest of the Nation. A State or territory identified as being the weak-link in the chain will draw terrorists and other bad actors to its territory, resulting in less security for all of us. While REAL ID does not create a national database or ID card, it addresses a national problem, the same problem recognized by the 9/11 Commission.

The 9/11 attacks cost 3,000 lives and $64 billion in immediate losses followed by longer-term financial losses of $375 billion. The potential for further loss of life and property far outweighs the financial burdens to States and territories in implementing REAL ID.

The Department has tried to address the financial burden on some stakeholders and we will continue to do that with the authority we have from our grant program. We have also sought to alleviate the time burden on some States and territories by announcing our extension policies in advance. However, these measures do not eliminate the security need for REAL ID to be implemented.

The Fraternal Order of Police supports implementation of the REAL ID Act, calling it "a common sense system that takes the right approach to ensuring the security and authenticity of the most commonly used identity document in the United States – a drivers' license."

To echo the words of the 9/11 Commission, "For terrorists, travel documents are as important as weapons." Our security as a nation is at stake, and I hope you will support the full implementation of REAL ID.

Thank you, Mr. Chairman, for the opportunity to appear before the Committee today. I would be delighted to answer any questions that the Committee may have.