

**Testimony
Darrell Williams
REAL ID Program Office Director**

**Before the
House of Representatives
Intergovernmental Affairs Committee**

01/23/2008

Chairman Thomas and distinguished Members of the Committee, thank you for the opportunity to appear before you today to discuss REAL ID.

As you may know, REAL ID is based on a recommendation of the 9/11 Commission. It is a recommendation to help deter future terrorist acts that the Department of Homeland Security (DHS) strongly supports. Further, one of Secretary Chertoff's priorities for 2008 is secure identification, and REAL ID is a core program within that objective. As we move forward this year, it is the Department's hope that States will work in partnership with us on this initiative.

On page 390 of the 9/11 Commission Report, it states:

“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 obtained 30 driver's licenses and state identification cards, some fraudulently. The hijacker who crashed American Airlines Flight 77 into the Pentagon, Hani Hanjour, had IDs from three states.

Quite simply, driver's licenses provide terrorists cover to operate within the United States. The U.S. intelligence community knows that fraudulent documents are integral to a terrorist's modus operandi. In fact, Mohammad Atta was an expert document forger trained by his superiors within al Qaeda and the hijackers used a total of 364 aliases, including different name spellings.

I am happy to report that the Department announced a final rule for REAL ID that took into account many of the inputs by States, driving down costs to States by 73%, all the while maintaining the homeland security objectives we originally set out to achieve.

The initial response to the final rule has been very favorable. As of today, 27 States, representing over half the U.S. population, have already requested extensions to work towards REAL ID compliance. And more are coming.

I would like to walk through a few different issue areas with you, including: requirements of the final rule and compliance timelines; funding; DMV database connectivity; and privacy improvements in the rule.

First, the requirements of the final rule. DHS recognized that despite a State's best intention not one could be compliant by the May deadline under the proposed rule. Therefore, States have been given the option to ask for an extension through December 31, 2009. During that time a series of 18 benchmarks must be met. Attached to my testimony is the list for your information. If States – who have acted in good faith and have achieved the 18 benchmarks – need a little extra time to become fully compliant, they can request a second extension until May 11, 2011. By this time, all States within the program must begin issuing fully compliant REAL ID licenses.

Another key element of the final rule – phased enrollment periods. Individuals born on or after December 1, 1964 desiring a REAL ID for official purposes will need to have the ID by December 1, 2014. All other persons will have until December 1, 2017. This approach gets secure credentials to those more likely to use fake IDs while making compliance by the States easier. Approximately 40% of the U.S. population will have until December 2017 to enroll, thus lowering the costs of the program substantially. As a result, States will not have to hire additional personnel or build additional facilities as projected earlier.

Now funding. As stated earlier, with the help of State stakeholders like the legislators, DHS developed a final rule at one-fourth the initial projected costs. The average increase per card issuance is about \$8. So, in Pennsylvania, with a four-year license that comes out to about an extra \$2 per year. Additionally, the Department currently has a grant announcement open in excess of \$80 million for REAL ID funding for States. Secretary Chertoff is also allowing each State to use up to 20% of its Homeland Security Grant funds for REAL ID compliance. States truly wishing to be compliant should be able to find additional monies in these grant funds.

DMV database connectivity. I'd like to start upfront by saying REAL ID is technically feasible. As you will see by the appended chart – "System Connectivity by State" – there is widespread activity being undertaken throughout the country by States to improve their standards for issuing ID cards. 47 of the States and the District of Columbia are connected to the SSOLV (Social Security On-Line Verification) database operated by the Social Security Administration. 28 States are signed up to use SAVE (Systematic Alien Verification for Entitlements), a DHS database, and most other States are entering into memoranda of understanding with DHS to begin this process. In FY06, participating State DMVs ran 1.2 million queries against the SAVE System. Three State DMVs and ten vital records agencies 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. Approximately 85% of the birth information dated back to 1935 is contained on this system. Finally, the State Department will be developing the system to permit DMVs to electronically verify 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 States on this important matter.

How does Pennsylvania fare with respect to DMV connectivity? Very good. Pennsylvania is connected to Social Security's database and is one of the 28 states with an MOU to check with DHS on lawful status. Connection to the database with birth certificate records, I'm pleased to announce is being paid by a DHS grant for all States.

Returning to the issue of Social Security number verification, a state audit report from 2007 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 were shown as deceased in SSA records. I'm sure Pennsylvanians would not want their SSNs used in a similar fashion and REAL ID will help ensure that it is not.

Now privacy. There have been concerns voiced about REAL ID creating a national identification card and national database. These concerns are simply not true. The final rule maintains the existing practices of how information is stored, collected and disseminated at the State and local level. The Federal government will not have any greater access to the information than it already does for law enforcement purposes. And as for a national ID card, driver's licenses will still be state issued. The final rule even allows flexibility in card design and security features used on the card.

At this time, I'd like to give you a line-item by line-item overview of the privacy improvements in the rule.

- 1) Name history not stored in Machine-Readable Zone (MRZ)
 - Offers greater protection by not having additional personal information beyond what is on the face of the card in the 2-dimensional barcode
- 2) Elimination of financial history check for DMV workers
 - Protects the privacy interests of DMV workers since their personal financial information is not exposed to their employers.
 - Eliminates potential union and legal issues
- 3) Greater ability to suppress address based on State law or court orders
 - Provides greater flexibility for States to protect confidential address information for protected classes (e.g., domestic violence victims)
 - Allows for display of alternative address, if permitted by State
- 4) States cannot phish for info in other State's database
 - Key measure to protect personal data from DMV workers
 - Prevents DMV workers from accessing information about people in another State without an authorized work reason

- Provides for audit and accountability
- 5) Data security and access addressed
 - Use of personal information must be consistent with Driver's Privacy Protection Act (DPPA)
 - Key provisions to ensure that the personal information provided to the DMV is not misused by DMV workers and cannot be hacked by outsiders
 - 6) Ability to redact birth certificate info
 - Protects personal information that is not necessary to establish an individual's name and date of birth.
 - 7) Privacy best practices to be published at same time as rule
 - Gives States a roadmap for additional privacy measures to take that are not required by REAL ID, but will enhance the privacy protections for the public.
 - 8) Issue of 3rd party skimming of data clearly raised for State action
 - Raises a key privacy issue that was outside the scope of the rulemaking so that States have options about how to address this issue.
 - 9) Consideration of encryption of MRZ down the road as technology improves
 - Ensures that future technology solutions can be used to enhance privacy without requiring DHS to go through a lengthy rulemaking process

Finally, let's take a moment to discuss a concern near and dear to the hearts of most Americans – identity theft. According to the Federal Trade Commission, there has been a 791% increase in reported instances of identity theft from 2000 to 2006. Now, REAL ID will make it much more difficult for fraudsters and identity thieves from stealing your identity. Instead of countless social security numbers being used to create false identities, there will be one record assigned to a driver's license. Despite the loyal opposition, led by the ACLU, asserting that there will be rampant increases in identity theft, common sense prevails...there will not. Only in Washington can a program designed to enhance the authentication of identity documents be construed as leading to more identity theft. The opposition is advocating insecure identification, not secure identification. And secure identification – that is, verifying that the identity documents make it into the right hands or that persons are, in fact, who they claim to be before issuing identity documents – equaling increased identity theft is a contradiction in terms. The Center for Identity Management and Information Protection based at Utica College conducted an analysis of Secret Service Identity theft cases that revealed 35% of the time a fraudulent driver's license was used. REAL ID will help combat identity theft. Period.

The Fraternal Order of Police supports REAL ID saying it's a public safety issue. Without secure identification, it "places both the officer and the public he is sworn to protect in greater danger." The Major County Sheriffs' Association supports REAL ID saying, "Secure and protected identification is critical in our efforts to keep our Country and its citizens safe." And most importantly, 82% of the American public say "favor"

when asked what they think about new rules for the issuance of driver's licenses designed to combat terrorism and identity theft (Public Opinion Strategies poll, September 2007).

To echo the words of the 9/11 Commission, "For terrorists, travel documents are as important as weapons." The National Intelligence Estimate from July provides a chilling reminder for the need to act now by concluding that al Qaeda was intensifying its efforts to place operatives inside the United States.

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.

Interim Benchmarks (Material Compliance Checklist)

Does the State:

1. Subject each applicant to a mandatory facial image capture and retain such image even if a drivers' license (DL) or identification card (ID) is not issued
2. Have each applicant sign a declaration under penalty of perjury that the information presented is true and correct, and retain this declaration pursuant to § 37.31.
3. Require an individual to present at least one of the source documents listed in subsections 37.11 (c)(1)(i) through (x) when establishing identity
4. Require documentation of:
 - Date of birth
 - Social Security Number
 - Address of principal residence
 - Evidence of lawful status
5. Have a documented exceptions process that meets the requirements established in 37.11(h)(1)-(3) (if States choose to have such a process)
6. Make reasonable efforts to ensure that the applicant does not have more than one DL or ID already issued by that State under a different identity
7. Verify lawful status through SAVE or another method approved by DHS
8. Verify Social Security account numbers with the Social Security Administration or another method approved by DHS
9. Issue DL and IDs that contain Level 1, 2 and 3 integrated security features
10. Surface (front and back) of cards include the following printed information in Latin alpha-numeric characters:
 - Full legal name
 - Date of birth
 - Gender
 - Unique DL/ID number
 - Full facial digital photograph
 - Address of principal residence [with exceptions]
 - Signature [with exceptions]
 - Date of transaction
 - Expiration date
 - State or territory of issuance
11. Commit to mark materially compliant DL and IDs with a DHS-approved security marking
12. Issue temporary or limited-term licenses to all individuals with temporary lawful status and tie license validity to the end of lawful status
13. Have a documented security plan for DMV operations in accordance with the requirements set forth in § 37.41
14. Have protections in place to ensure the security of personally identifiable information
15. Require all employees handling source documents or issuing DLs or IDs to attend and complete the AAMVA approved (or equivalent) fraudulent document recognition training and security awareness training
16. Conduct name-based and fingerprint-based criminal history and employment eligibility checks on all employees in covered positions or an alternative procedure approved by DHS
17. Commit to be in material compliance with Subparts A through D no later than January 1, 2010 or within 90 days of submission of this document, whichever date is earlier
18. Clearly state on the face of non-compliant DLs or IDs that the card is not acceptable for official purposes, except for licenses renewed or reissued under § 37.27